DATA DATA

DATENMANAGEMENT UND DATENSCHUTZPOLITIK

INHALTSVERZEICHNIS

13. die Lobbyarbeit

14. die Verarbeitung personenbezogener Daten zu anderen Zwecken als denen, für die sie erhoben wurden

TEIL V: BESCHÄFTIGUNGSBEZOGENE VERARBEITUNG

15. arbeitsrechtliche und personelle Unterlagen

16. die Verarbeitung von Daten im Zusammenhang mit Eignungstests

17. die Verwaltung von Lebensläufen

18. die Datenverarbeitung im Zusammenhang mit der Überwachung der elektronischen Post

19. die Datenverarbeitung im Zusammenhang mit der Kontrolle von IT-Tools

20. die Datenverarbeitung zum Zwecke der Überwachung der Internetnutzung am Arbeitsplatz

21. die Datenverarbeitung im Zusammenhang mit der Kontrolle der Nutzung von Firmenhandys

22. die Datenverarbeitung im Zusammenhang mit der Nutzung des Navigationssystems

23. die Verarbeitung von Daten im Zusammenhang mit der Videoüberwachung am Arbeitsplatz

24. die Verarbeitung von Daten über Studienverträge

TEIL VI: ZUSTIMMUNG DER BETROFFENEN PERSON

25. die Verarbeitung von Daten im Zusammenhang mit dem Besuch der Website

26. auf der Website registrieren

27. die Verarbeitung der bei Veranstaltungen aufgenommenen Bilder

VII. VERTRAG ALS RECHTSGRUNDLAGE FÜR DIE VERARBEITUNG

28 Verarbeitung von Daten der Vertragsparteien

29 Kontaktangaben der Partner der juristischen Person

TEIL VIII - VERARBEITUNG AUF DER GRUNDLAGE RECHTLICHER VERPFLICHTUNGEN

30. die Verarbeitung von Daten zum Zweck der Erfüllung von Steuer-, Beitrags- und Buchführungspflichten

31. beschäftigungsbezogene Datenverarbeitung

32. die Verarbeitung von Zahlerdaten

56 Recht auf Rechtsbehelf gegen den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter

TEIL XIII - SCHLUSSBESTIMMUNGEN

57. die Aufstellung, Änderung und Einarbeitung der Geschäftsordnung

ANNEXEK

Anhang 1: Datenverwaltungsregister

Anhang 2: Register der Datenschutzvorfälle

Anhang 3: Der allgemeine Datenschutzhinweis des Unternehmens

Anhang 4: Einverständniserklärung

Anhang 5: Ausleihe von Dokumenten

Anhang 6: Inspektionsprotokoll

Anhang 7: Informationen für Arbeitnehmer

Anhang 8 Informationen über die Eignungsprüfung

Anhang 9 Protokoll über die Vernichtung von Lebensläufen

Anhang 10 Informationen zur Kamera

Anhang 11 - Vertragliche Informationen zur Datenverarbeitung

Anhang 12 Cookie-Informationen

Anhang 14 Erklärung über den Zugang zu den Regeln und die Vertraulichkeit

15. Vorfallsbericht

Anhang 16 Allgemeine Vertragsbedingungen für die Datenverarbeitung

Anhang 17 Klausel im Arbeitsvertrag

PREAMBULUM

(1) Die D&D GmbH (nachfolgend "das Unternehmen" genannt) verpflichtet sich, bei ihrer Tätigkeit die Vorschriften des Datenschutzes und der Datensicherheit einzuhalten. In Ergänzung zu den derzeit geltenden Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und

zur Aufhebung der Verordnung (EG) Nr. 95/46/EG (nachfolgend "DSGVO" genannt) und des Gesetzes CXII von 2011 über das Recht auf informationelle Selbstbestimmung und Informationsfreiheit (nachfolgend "Gesetz über die Informationsgesellschaft" genannt) erlässt die Geschäftsführung des Unternehmens diese Datenschutz- und Datensicherheitsrichtlinie (nachfolgend "Richtlinie" genannt). Die Richtlinie tritt am Tag nach ihrer Verabschiedung in Kraft und wird den Mitarbeitern des Unternehmens und denjenigen, die mit dem Unternehmen in vertraglichen Beziehungen stehen, bekannt gemacht, soweit sie davon betroffen sind.

(2) Das Unternehmen übt Transport-, Speditions- und Lagertätigkeiten aus und erbringt Dienstleistungen. Das Unternehmen beschäftigt zum Zeitpunkt der Verabschiedung dieser Vorschriften Mitarbeiter, so dass auch die damit verbundene Datenverarbeitung durch diese Vorschriften geregelt wird. Neben der papiergestützten Datenverwaltung und -aufzeichnung verwaltet und speichert das Unternehmen auch Daten in elektronischer Form und hält die in dieser Richtlinie festgelegten Anforderungen an die Datensicherheit ein.

(3) Das Unternehmen verwendet die Buchhaltungssoftware Novitax, die Online-Zeiterfassungssoftware OLM, die Lager- und Transportverwaltungssoftware Transorg und die Fahrzeugverfolgungssoftware WebEye, wobei die Softwareentwickler (in der Reihenfolge Novitax Kft., Kulcs-Soft Computer Technology Plc., Transorg Kft. und WebEye Hungary Kft.

(4) Das Unternehmen stellt den Betrieb seiner IT-Ausstattung und seines Netzwerks sicher (Serveraufbau, Softwareinstallation, Konfiguration, Fehlerbehebung, Sicherheitsüberwachung). Das Unternehmen sorgt für einen angemessenen Virenschutz, eine Firewall, Backups und einen unterbrechungsfreien Betrieb. IT-Geräte sind passwortgeschützt, und das Unternehmen bemüht sich um die Verschlüsselung tragbarer IT-Geräte und elektronischer Kommunikation.

(5) Das Unternehmen kategorisiert, klassifiziert oder verarbeitet keine Daten über seine Kunden, Mitarbeiter oder Personen, die in einem Rechtsverhältnis zu ihm stehen.

(6) Gemäß Artikel 25 DSGVO müssen die Datenschutzgrundsätze bei allen Tätigkeiten und Entscheidungen des Unternehmens angewandt werden, und das Unternehmen bemüht sich, so weit wie möglich eine Datenschutz-IT-Lösung und organisatorische Vorkehrungen anzuwenden, die den Schutz der Daten auf die wirksamste Weise nach dem Stand der Technik gewährleisten.

(7) Alle Datenschutzprozesse des Unternehmens müssen geregelt, transparent, nachvollziehbar und einem bestimmten Auftrag zuzuordnen sein.

(8) Das Unternehmen wird sich bemühen, personenbezogene Daten nicht zu verarbeiten, wenn es möglich ist, einen bestimmten Zweck ohne die Verarbeitung personenbezogener Daten zu erreichen.

(9) Das Unternehmen organisiert seine Mitarbeitertätigkeit so, dass möglichst wenige Mitarbeiter personenbezogene Daten verarbeiten und der Mitarbeiter, der die personenbezogenen Daten verarbeitet, eine Gruppe von personenbezogenen Daten (z.B. Personaldaten, Zahlungsdaten, Kundenbeziehungsdaten) verarbeitet.

TEIL I

Allgemeine Bestimmungen

1) Ziel der Verordnung

Die Datenschutz- und Datensicherheitspolitik des Unternehmens (nachstehend "Politik" genannt) soll die Anforderungen an den Datenschutz und die Datensicherheit festlegen, um die unbefugte Nutzung personenbezogener Daten im Rahmen der Tätigkeit des Unternehmens zu verhindern und einen angemessenen Schutz der Rechte der betroffenen Personen zu gewährleisten.

(2) Zweck des Kodex ist es, interne Regeln und Maßnahmen festzulegen, die sicherstellen, dass die Datenverarbeitung und die Datenverwaltung des Unternehmens mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 29. Juni 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 95/46/EG (Datenschutz-Grundverordnung, im Folgenden "DSGVO") (2016. 27. April 2011) - und die Bestimmungen des Gesetzes CXII von 2011 über das Recht auf informationelle Selbstbestimmung und Informationsfreiheit (im Folgenden "Infotv.").

(3) In Angelegenheiten, die nicht durch diese Richtlinie abgedeckt sind, gelten die Bestimmungen der Datenschutz-Grundverordnung und des Informationsgesetzes.

(4) Der Geltungsbereich dieser Richtlinie erstreckt sich auf die Verarbeitung personenbezogener Daten natürlicher Personen durch das Unternehmen, wobei Selbständige, Einzelunternehmer, Einzelunternehmen, Kunden und Lieferanten als natürliche Personen im Sinne dieser Richtlinie gelten.

(5) Der Anwendungsbereich der Richtlinie erstreckt sich nicht auf die Verarbeitung personenbezogener Daten von juristischen Personen, ihren Namen, ihre Form und ihre Kontaktdaten.

2. auslegende Bestimmungen

(6) Für die Zwecke dieser Richtlinie haben die in Artikel 4 der Datenschutz-Grundverordnung definierten Begriffe die folgenden zusätzlichen Bedeutungen:

7) Datensicherheit: die Gesamtheit der organisatorischen, technischen Lösungen und Verfahrensregeln, die verhindern können, dass ein Datenschutzvorfall eintritt; der Zustand der Datenverwaltung, in dem die organisatorischen, technischen Lösungen und Maßnahmen die Risikofaktoren und damit die Bedrohung minimieren.

8. Datenverarbeitungsregister: ein gemäß Artikel 30 der DSGVO geführtes Register der Verarbeitungen personenbezogener Daten, das alle relevanten Informationen über die Verarbeitung der betreffenden Daten enthält, Anhang 1 dieser Richtlinie.

9. Register für Datenschutzvorfälle: das gemäß Artikel 33 Absatz 5 der Datenschutz-Grundverordnung geführte Register, das in Anhang 2 dieser Strategie aufgeführt ist.

10. personenbezogene Daten von Mitarbeitern: personenbezogene Daten von Personen, die in einem Arbeitsverhältnis oder einem vereinfachten Arbeitsverhältnis mit dem Unternehmen stehen, die unter Beachtung des Grundsatzes der Zweckbindung verarbeitet werden.

11. personenbezogene Datenverwaltung zu Registerzwecken: eine nach bestimmten Kriterien strukturierte Papier- oder elektronische Datei aus nach vorgegebenen Kriterien erhobenen personenbezogenen Datenarten, in der die Auffindbarkeit und Wiederauffindbarkeit von Daten anhand verschiedener Merkmale während der Dauer der Datenverwaltung gewährleistet ist. Eine Datenverarbeitung für Zwecke des Registers liegt auch dann vor, wenn die Daten aus der Kundenbeziehungspflege vor der Eintragung des Registers stammen, die Verarbeitung der Daten aber vom Zweck der Verarbeitung her vom Basisprozess getrennt ist. Die Verarbeitung zum Zweck der Registerführung muss ebenfalls mit den Grundsätzen und Bestimmungen der DSGVO übereinstimmen.

12. die Verarbeitung personenbezogener Daten zum Zwecke der Fallbearbeitung: die Verarbeitung personenbezogener Daten, die das Unternehmen einem anderen für die Verarbeitung Verantwortlichen zur Ausübung öffentlicher Gewalt (Genehmigung einer Tätigkeit) zur Verfügung stellt. Die Fallbearbeitung ist eng mit der Bearbeitung eines Falles verbunden, wobei ihr Hauptzweck darin besteht, die Daten bereitzustellen, die für die Durchführung der den Fall betreffenden Verfahren, die Identifizierung der Verfahrensbeteiligten und den Abschluss des Falles erforderlich sind. Für die Verarbeitung zum Zwecke der Fallbearbeitung werden personenbezogene Daten nur in die Akte des Falles aufgenommen und dürfen nur zu diesem Zweck verarbeitet werden, bis die zugrunde liegende Akte beseitigt ist.

TEIL II

Haftungsregelung für den Datenschutz

3 Stufen der Verarbeitung

13. das Unternehmen steht in Kontakt mit Datenverarbeitern, die es auswählt, um das höchstmögliche Niveau an Datenschutz- und Datensicherheitslösungen zu gewährleisten; zu diesem Zweck hat es vorab Kenntnis von den Datenschutz- und Datensicherheitsrichtlinien der Datenverarbeiter, und die entsprechenden organisatorischen und IT-Sicherheitsbestimmungen sind im Datenverarbeitungsvertrag festgelegt.

(14) Das Unternehmen stellt sicher, dass die Datenverarbeiter so weit wie möglich nicht mit den personenbezogenen Daten von Beschäftigten und Kunden in Berührung kommen; lässt sich dies nicht vermeiden, so kann die Übermittlung dieser Daten in elektronischer oder Papierform im Rahmen geeigneter Sicherheitsmaßnahmen erfolgen.

4. die Zuständigkeiten des Leiters des Controllers

(15) Für die Zwecke der Anwendung der Datenschutzbestimmungen gilt der Geschäftsführer des Unternehmens als der für die Verarbeitung Verantwortliche.

16 Der Leiter des für die Datenverarbeitung Verantwortlichen ist verantwortlich für:

a) für die Einrichtung und den Betrieb des institutionellen Datenschutz- und Datensicherheitssystems des Unternehmens, wobei er die in seine Zuständigkeit fallenden Maßnahmen ergreift, um die erforderlichen personellen, materiellen und technischen Voraussetzungen für den Schutz der von der Stelle verarbeiteten personenbezogenen Daten zu gewährleisten;

(b) die Datenschutzerziehung und -schulung der Mitarbeiter;

c) zur regelmäßigen datenschutzrechtlichen Überwachung der Tätigkeiten des von ihm geleiteten oder kontrollierten Unternehmens, zur Beseitigung der bei der Überwachung festgestellten Mängel oder rechtswidrigen Umstände, zur Einleitung oder Durchführung der erforderlichen Verfahren zur Feststellung der persönlichen Haftung;

d) Gewährleistung der für die Ausübung der Rechte der betroffenen Personen erforderlichen Bedingungen.

(e) die Auswahl, Beschäftigung oder Ernennung eines Datenschutzbeauftragten.

(17) Die Haftung des für die Verarbeitung Verantwortlichen schließt die Haftung von Personen, die mit dem Unternehmen verbunden sind, weder auf Schadensersatz noch auf strafrechtliche Haftung aus.

Ist das Unternehmen aufgrund einer Verletzung des Schutzes personenbezogener Daten zur Zahlung von Schadenersatz oder Entschädigung verpflichtet, müssen alle Anstrengungen unternommen werden, um die Person zu ermitteln, die die Verletzung des Schutzes personenbezogener Daten tatsächlich begangen hat, und, falls dies gelingt, ein Schadenersatzverfahren gegen sie einzuleiten.

5 Aufgaben und Befugnisse des Leiters des für die Verarbeitung Verantwortlichen

19 Aufgaben und Befugnisse des Leiters des für die Verarbeitung Verantwortlichen:

a) die Konzeption, die Verwaltung und den ordnungsgemäßen Betrieb aller Datenverwaltungssysteme (Register, Datenspeicher, Arbeitsabläufe, Informationsflüsse und -verarbeitung, Berechtigungen), für die er verantwortlich ist, mit der vollen Verantwortung für die Durchsetzung der Gesetze und Vorschriften über die Verarbeitung personenbezogener Daten.

(b) die Verhinderung des unbefugten Zugriffs auf personenbezogene Daten und ihrer unbefugten Weitergabe, Veränderung oder Löschung, den technischen Schutz und, sofern gesetzlich nicht anders vorgesehen, die Wahrung der Rechte der betroffenen Person bei der Verarbeitung personenbezogener Daten durch den für die Verarbeitung Verantwortlichen zu gewährleisten, um den Schutz personenbezogener Daten zu gewährleisten.

c) ist persönlich verantwortlich für die Tätigkeiten des Unternehmens und seiner Auftragnehmer, für das rechtmäßige und ordnungsgemäße Funktionieren des Unternehmens, einschließlich der Tätigkeiten des für die Datenverarbeitung Verantwortlichen des Personals, für die Einhaltung der Datenschutzvorschriften und der damit verbundenen Verwaltungsvorschriften.

d) die Überwachung der praktischen Umsetzung der Sicherheitsvorschriften und die Ergreifung von Maßnahmen zur Behebung etwaiger Unzulänglichkeiten;

e) Festlegung der organisatorischen und betrieblichen Voraussetzungen für die Datenverarbeitung, Gewährleistung der Durchsetzung der betrieblichen Anforderungen und der Anforderungen an die Datensicherheit;

f) zur Feststellung und Kontrolle der Ordnungsmäßigkeit und Dokumentation der Datenverarbeitung;

(g) die Risiken für den Datenschutz zu analysieren und eine Folgenabschätzung vorzunehmen.

h) sicherzustellen, dass Aufzeichnungen über die Datenverarbeitung und über Datenschutzvorfälle geführt und auf dem neuesten Stand gehalten werden.

6. der Datenschutzbeauftragte des Unternehmens

(20) Der Datenschutzbeauftragte des Unternehmens ist, sofern er nicht angestellt ist, ein vertraglich gebundener Auftragnehmer, der fachlich kompetent ist, über Fachkenntnisse des Datenschutzrechts und der Datenschutzpraxis verfügt und in der Lage ist, die Aufgaben zu erfüllen.

(21) Wenn das Unternehmen einen Datenschutzbeauftragten beschäftigt, muss dessen Stellenbeschreibung die Aufgaben im Zusammenhang mit dem Datenschutz enthalten.

(22) Das Unternehmen darf den DSB im Zusammenhang mit der Wahrnehmung seiner Aufgaben nicht entlassen oder bestrafen. Der DSB ist unmittelbar dem Hauptgeschäftsführer des Unternehmens unterstellt.

23. dem Datenschutzbeauftragten des Unternehmens, im Rahmen seiner Aufgaben:

a) Verwaltung der Datenschutzaktivitäten des Unternehmens, Bereitstellung von Informationen, professioneller Beratung und Anleitung;

(b) an Entscheidungen im Zusammenhang mit der Datenverarbeitung mitzuwirken oder diese zu unterstützen und die Rechte der betroffenen Personen zu gewährleisten;

c) Überwachung der Einhaltung der Rechtsvorschriften über die Datenverwaltung, der internen Datenschutz- und Datensicherheitspolitik und der Anforderungen an die Datensicherheit;

d) die bei ihr eingehenden Meldungen zu untersuchen und, falls ein Datenschutzvorfall festgestellt wird, den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter aufzufordern, den Vorfall zu beheben, in begründeten Fällen eine Untersuchung mit dem Leiter des Unternehmens einzuleiten und Empfehlungen abzugeben, um die nachteiligen Folgen des Vorfalls zu beheben und ähnliche Vorfälle in Zukunft zu verhindern;

e) Ausarbeitung von Entwürfen für Arbeitgeberregelungen zum Datenschutz, Mitwirkung bei der Ausarbeitung anderer Regelungen zum Datenschutz. Unterstützung des CEO bei der Durchsetzung von Gesetzen und Vorschriften über die Datenverarbeitung, indem er Änderungen der Datenschutzgesetze verfolgt und den CEO auf die Notwendigkeit einer Änderung des Arbeitgeberreglements hinweist;

f) Unterstützung bei der Ausbildung und erforderlichenfalls bei der Prüfung der vom Unternehmen beschäftigten Personen;

(g) Unterstützung bei der Entwicklung einer einheitlichen Praxis durch die Ausarbeitung von Stellungnahmen in Einzelfällen;

h) Er entwickelt den Standpunkt des Unternehmens zu Fragen, die seine Datenverwaltungstätigkeiten betreffen, steht in Verbindung mit dem NAIH, trägt zur Durchführung der Untersuchungen des NAIH bei und beantwortet diesbezügliche Anfragen;

(i) die Antwort auf den Antrag der betroffenen Person auf Verarbeitung ihrer personenbezogenen Daten vorzubereiten;

j) sicherzustellen, dass die Datenschutzerklärung, die Datenschutzpolitik und der Datenschutzhinweis auf der Website des Unternehmens auf dem neuesten Stand gehalten werden;

(k) bei Rechtsstreitigkeiten die Position des Unternehmens zum Datenschutz mit der Person zu koordinieren, die das Unternehmen in Rechtsstreitigkeiten vertritt. Er kann als Sachverständiger an Rechtsstreitigkeiten über den Datenschutz teilnehmen;

(l) einen Jahresbericht über die im Falle der Verarbeitung personenbezogener Daten abgelehnten Auskunftsersuchen zu erstellen;

m) die Datenschutzaktivitäten des Unternehmens in einem jährlichen Bericht an die Unternehmensleitung zu bewerten, sofern dies gewünscht wird;

n) eine Stellungnahme zu den Vorschlägen für die Entwicklung von IT-Aufzeichnungen und Software, die personenbezogene Daten enthalten, unter dem Gesichtspunkt des Datenschutzes abzugeben;

o) in Ausübung seiner Pflichten und Befugnisse - vorbehaltlich des Grundsatzes der Zweckbindung - das Recht hat, die vom Unternehmen durchgeführte Datenverarbeitung zu überprüfen und vom für die Verarbeitung Verantwortlichen Informationen zu verlangen;

p) Überwachung der Einhaltung der Datenschutz-Grundverordnung und anderer Datenschutzvorschriften der EU und der Mitgliedstaaten, dieser internen Vorschriften, Schulungen und Audits;

q) bei der Überwachung des Zugangs und der Zugangsrechte mitzuwirken;

(r) fachliche Beratung bei der Folgenabschätzung, Überwachung der Durchführung der Folgenabschätzung.

(s) Er überwacht die Einhaltung der Verpflichtungen der Datenverarbeiter aus dem Datenverarbeitungsvertrag und meldet dem Unternehmensleiter, wenn er vertragswidrige Praktiken feststellt, und schlägt die Beendigung des Vertragsverhältnisses vor.

TEIL III

Schutz der personenbezogenen Daten im Unternehmen

7 Grundregeln für die Datenverarbeitung

Die vom Unternehmen verarbeiteten Daten müssen durch geeignete Maßnahmen geschützt werden, insbesondere gegen unbefugten Zugriff, Veränderung, Weitergabe, Veröffentlichung, Löschung oder Vernichtung, zufällige Zerstörung oder Beschädigung sowie gegen Unzugänglichkeit infolge von Änderungen der verwendeten Technologie.

25 Das Unternehmen setzt die technischen und organisatorischen Maßnahmen durch und legt die Verfahrensregeln fest, die zur Durchsetzung der DSGVO und des Informationsgesetzes bei all seinen Datenverarbeitungsaktivitäten erforderlich sind, um die Sicherheit personenbezogener Daten zu gewährleisten, wie im Kodex und anderen internen Vorschriften und anderen Dokumenten (Prozesse, Arbeitsverträge, Stellenbeschreibungen) und Managementmaßnahmen festgelegt.

(26) Der für die Verarbeitung Verantwortliche hat die Verarbeitungsvorgänge so zu gestalten und durchzuführen, dass der Schutz der Privatsphäre der betroffenen Personen und die Möglichkeit zur Ausübung ihrer Rechte gewährleistet sind. Das Unternehmen unterwirft die Verarbeitung personenbezogener Daten einer Geheimhaltungspflicht, die in Anhang 17 dargelegt ist.

27 Der Zugang zu den personenbezogenen Daten wird vom Unternehmen mit elektronischen Mitteln (Netzlaufwerk, Zugangskontrollsystem) durch die Festlegung von Berechtigungsstufen eingeschränkt.

(28) Nur die betreffenden Sachbearbeiter haben Zugang zu den Dokumenten, die im Rahmen der Arbeit oder der Bearbeitung anfallen, und die Dokumente, die Lohn- und Gehaltsabrechnungen, Beschäftigungsdaten oder andere personenbezogene Daten enthalten, sind in verschließbaren Büros und Schränken sicher aufzubewahren.

(29) Der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter hat im Rahmen seiner Tätigkeit die Sicherheit der Daten zu gewährleisten. Das Unternehmen trifft unter Berücksichtigung des Stands von Wissenschaft und Technik und der Implementierungskosten, des Umfangs, der Umstände und der Zwecke der Art der Verarbeitung sowie des Risikos für die Rechte und Freiheiten natürlicher Personen die technischen und organisatorischen Maßnahmen und legt die Verfahrensvorschriften fest, die zur Durchsetzung der Datenschutzgrundsätze, -vorschriften und -garantien zum Schutz der Rechte der betroffenen Personen erforderlich sind. Unter mehreren möglichen Datenverarbeitungslösungen sollte nach Möglichkeit diejenige gewählt werden, die ein höheres Schutzniveau für personenbezogene Daten gewährleistet.

(30) Zum Schutz der in den verschiedenen Registern gespeicherten elektronisch verarbeiteten Daten muss eine geeignete technische Lösung gewährleisten, dass die in den Registern gespeicherten Daten nicht direkt mit der betroffenen Person verknüpft und ihr zugeordnet werden können, es sei denn, dies ist gesetzlich zulässig.

31 Das Unternehmen führt eine automatisierte Verarbeitung von personenbezogenen Daten durch. Während der automatisierten Verarbeitung ergreifen der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter zusätzliche Maßnahmen, um sicherzustellen:

a) Unterrichtung der betroffenen Person;

b) die Genauigkeit und das ordnungsgemäße Funktionieren des Geräts;

c) Verhinderung der Eingabe von Daten durch Unbefugte;

(d) Verhinderung der Benutzung von automatischen Datenverarbeitungsanlagen durch Unbefugte mittels Datenübertragungseinrichtungen;

(e) die Überprüfbarkeit und Feststellbarkeit, ob personenbezogene Daten mit Hilfe von Datenübertragungseinrichtungen übermittelt worden sind oder übermittelt werden können;

(f) die Überprüfbarkeit und Feststellbarkeit, welche personenbezogenen Daten wann und von wem in automatisierte Datenverarbeitungssysteme eingegeben worden sind;

(g) die Wiederherstellbarkeit der installierten Systeme im Falle eines Ausfalls;

h) Meldung von Fehlern bei der automatisierten Verarbeitung;

(i) Die betroffene Person muss die Möglichkeit haben, sich einzumischen, ihre Meinung zu äußern und Einwände gegen die Entscheidung zu erheben.

8. grundsätzliche Regeln für den Datenschutz

(32) Für das Gebäude, in dem personenbezogene Daten verarbeitet werden, muss ein angemessener physischer Schutz und Brandschutz gewährleistet sein. Nur befugte Personen haben Zugang zu den verschließbaren Räumen, in denen personenbezogene Daten verarbeitet werden.

(33) Das Unternehmen gewährleistet den Schutz der IT-Systeme durch Firewalls, den Schutz vor Viren, die Sicherung personenbezogener Daten auf Datenträgern, den Schutz von Benutzernamen und Passwörtern und die Verschlüsselung mobiler Datenträger.

34 Das nicht im Büro tätige Personal (z. B. Reinigungs- und Wartungspersonal) darf nicht mit personenbezogenen Daten in Berührung kommen; daher sind Dokumente mit solchen Daten in einem abschließbaren Schrank aufzubewahren, Monitore sind vor Blicken zu schützen, und das Display ist abzuschließen und mit einem Passwort zu schützen, wenn das IT-Gerät unbeaufsichtigt bleibt.

35 Das Unternehmen wird seine IT-Systeme monatlich aktualisieren und kann sie mit nicht realen Daten testen. Das Unternehmen wird rechtzeitig vor der Installation oder Aktualisierung von IT-Programmen benachrichtigt, um sicherzustellen, dass der Zugriff auf personenbezogene Daten zu jeder Zeit gewährleistet ist.

36 Mitarbeiter des Unternehmens, die eine bestimmte Kategorie personenbezogener Daten (z. B. Mitarbeiterdaten, Finanzdaten von Mitarbeitern, Kundendaten) nicht verarbeiten, sollten keinen Zugang zu diesen Daten haben.

37 Es macht es auch für Benutzer mit Administratorrechten nachvollziehbar, alle Datenverwaltungsvorgänge einer Person zuzuordnen (z.B. admin1, admin2, admin3 mit Benutzernamen).

38 Die im Unternehmen eingesetzte Software für die elektronische Datenverarbeitung und -aufzeichnung ermöglicht die Protokollierung des Systems, so dass festgestellt werden kann, welcher Benutzer wann was aufgezeichnet oder gelöscht hat. Das Unternehmen verwendet nur Originalsoftware und lässt sich für die verwendete Software eine Folgenabschätzung ausstellen.

39 Das Unternehmen kauft nach Ablauf der Garantiezeit neue Datenträger für Hardware und vernichtet Datenträger, die die Garantiezeit überschreiten.

40 Das Unternehmen stellt sicher, dass sowohl die elektronische als auch die papiergestützte ein- und ausgehende Kommunikation kontrolliert wird.

41 Bei der Verwendung von Passwörtern muss darauf geachtet werden, dass nicht zwei Personen dasselbe Passwort haben und dass die Benutzer die Passwörter der anderen nicht kennen.

42 Beim Scannen sollte darauf geachtet werden, dass jeder Benutzer Dokumente, die persönliche Daten enthalten, in seinem eigenen Ordner speichern kann.

(43) Papierdokumente, die personenbezogene Daten enthalten, dürfen nur mit Genehmigung des Geschäftsführers aus den Räumlichkeiten des Unternehmens entfernt oder von dem in Anhang 1 angegebenen Ort an einen anderen Ort verbracht werden. Anhang 5 ist auszufüllen, um die Verbringung des Dokuments zu dokumentieren.

9. die Datenschutzpolitik des Unternehmens

44 Die allgemeinen Datenverwaltungsinformationen des Unternehmens sind in Anhang 3 aufgeführt.

45 Führt das Unternehmen Ad-hoc-Verarbeitungen durch (z. B. Organisation einer Veranstaltung, Stellenausschreibung), so stellt es sicher, dass die entsprechenden Informationen erstellt und den betroffenen Personen zur Verfügung gestellt werden. Das Unternehmen holt vor der Ad-hoc-Verarbeitung die Stellungnahme des DSB ein.

TEIL IV

MÖGLICHE RECHTSGRUNDLAGEN FÜR DIE VERARBEITUNG

(46) Das Unternehmen stellt sicher, dass die Rechte der betroffenen Person bei allen seinen Verarbeitungen grundsätzlich unentgeltlich ausgeübt werden.

10. die Zustimmung der betroffenen Person

(47) Beruht die Verarbeitung personenbezogener Daten auf einer Einwilligung, so wird die Einwilligung der betroffenen Person eingeholt, indem die Informationen und der Inhalt des Datenanforderungsformulars gemäß Anhang 4 vorgelegt werden. Die Einwilligung muss freiwillig gegeben werden

(48) Die Einwilligung gilt auch dann als erteilt, wenn die betroffene Person beim Besuch der Website des Unternehmens ein zu diesem Zweck geschaffenes Kästchen ankreuzt, aus dem im jeweiligen Kontext eindeutig hervorgeht, dass die betroffene Person freiwillig und in Kenntnis der Sachlage in die beabsichtigte Verarbeitung ihrer personenbezogenen Daten einwilligt. Schweigen, das Ankreuzen eines Kästchens oder Untätigkeit gelten nicht als Einwilligung.

Die Einwilligung gilt für alle Verarbeitungstätigkeiten für denselben Zweck oder dieselben Zwecke. Erfolgt die Verarbeitung zu mehreren Zwecken gleichzeitig, muss die Einwilligung für alle Verarbeitungszwecke erteilt werden.

50. Bezieht sich die Einwilligung der betroffenen Person auch auf andere Angelegenheiten, insbesondere den Abschluss eines Kauf- oder Dienstleistungsvertrags, so muss die Einwilligung in einer von diesen anderen Angelegenheiten klar unterscheidbaren Weise in verständlicher und leicht zugänglicher Form und in klarer und einfacher Sprache ausgedrückt werden. Jeder Teil der Einwilligungserklärung der betroffenen Person, der gegen die DSGVO verstößt, ist nicht verbindlich.

(51) Das Unternehmen darf den Abschluss oder die Erfüllung eines Vertrages nicht von der Bereitstellung personenbezogener Daten abhängig machen, die für die Erfüllung des Vertrages nicht erforderlich sind.

(52) Der Widerruf der Einwilligung ist auf die gleiche Weise möglich wie die Erteilung der Einwilligung. Um den Newsletter abzubestellen, muss ein Link am Ende jedes Newsletters die Möglichkeit bieten, die Einwilligung zu widerrufen.

(53) Wurden die personenbezogenen Daten mit Einwilligung der betroffenen Person erhoben, so kann der für die Verarbeitung Verantwortliche sie zur Erfüllung einer rechtlichen Verpflichtung, der die betroffene Person unterliegt, ohne weitere ausdrückliche Einwilligung verarbeiten, es sei denn, das Gesetz sieht etwas anderes vor, und zwar auch dann, wenn die Einwilligung widerrufen wurde.

54 Das Unternehmen muss jederzeit nachweisen können, dass die betroffene Person ihre Einwilligung zu der Verarbeitung gegeben hat.

11. der Vertrag als Rechtsgrundlage

(55) Bei der Vorbereitung des Vertrags, bei der Ausarbeitung des Entwurfs und bei der Übermittlung des Entwurfs zur Stellungnahme dürfen keine personenbezogenen Daten angegeben werden.

(56) Es dürfen nur personenbezogene Daten verarbeitet werden, die für die Gültigkeit und Erfüllung des Vertrags erforderlich sind.

57 Verträge sollten eine spezielle Datenschutzklausel enthalten, in der die Maßnahmen zum Schutz der personenbezogenen Daten, die Gegenstand des Vertrags sind, auf Papier und in elektronischer Form festgelegt sind.

(58) Die Verarbeitung der personenbezogenen Daten, die Gegenstand des Vertrages sind, kann während der Laufzeit des Vertrages erfolgen. Sie dürfen auch noch 5 Jahre nach Erfüllung oder Beendigung des Vertrags verwendet werden, um etwaige Ansprüche aus dem Vertrag gegenseitig nachzuweisen oder durchzusetzen. Erstreckt sich die vertragliche Gewährleistung über 5 Jahre nach der Vertragserfüllung hinaus, können die im Vertrag enthaltenen personenbezogenen Daten noch 5 Jahre nach Ablauf der Gewährleistungsfrist rechtmäßig verarbeitet werden.

59 Das Unternehmen informiert den Vertragspartner über die in dieser Richtlinie dargelegten Datenverarbeitungs- und Datenschutzbedingungen, die für den Vertragsabschluss relevant sind.

12. die Erfüllung einer rechtlichen Verpflichtung

60 Die Regeln für die Datenverarbeitung auf der Grundlage gesetzlicher Verpflichtungen - Zweck der Datenverarbeitung, Umfang der verarbeiteten Daten, Dauer der Speicherung, Empfänger - richten sich nach den Bestimmungen des geltenden Rechts.

(61) Die Verarbeitung aufgrund einer rechtlichen Verpflichtung erfolgt unabhängig von der Einwilligung der betroffenen Person. In solchen Fällen ist die betroffene Person vor Beginn der Verarbeitung über den zwingenden Charakter der Verarbeitung zu unterrichten und ihr sind alle Fakten im Zusammenhang mit der Verarbeitung ihrer Daten klar und ausführlich darzulegen, insbesondere die Zwecke und die Rechtsgrundlage der Verarbeitung, die Identität des für die Verarbeitung Verantwortlichen und des Auftragsverarbeiters, die Dauer

der Verarbeitung, die Tatsache, dass der für die Verarbeitung Verantwortliche ihre personenbezogenen Daten aufgrund einer rechtlichen Verpflichtung verarbeitet, der die betroffene Person unterliegt, sowie die Personen, die Zugang zu den Daten haben können. Die Informationen sollten auch die Rechte und Rechtsbehelfe der betroffenen Person im Zusammenhang mit der Verarbeitung umfassen. Im Falle einer obligatorischen Verarbeitung können die Informationen auch durch einen Verweis auf die Rechtsvorschriften, die die vorgenannten Informationen enthalten, veröffentlicht werden.

13. die Lobbyarbeit

(62) Personenbezogene Daten können auch verarbeitet werden, wenn dies zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich ist.

Die Weiterverarbeitung von Kundendaten und Beschäftigtendaten kann auf dieser Rechtsgrundlage erfolgen, doch muss vor der Verarbeitung auf dieser Rechtsgrundlage geprüft werden, ob die betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten vernünftigerweise erwarten konnte, dass eine Verarbeitung für die Zwecke, für die die Daten erhoben wurden, stattfinden würde.

(64) Die Verarbeitung personenbezogener Daten zu Zwecken der Direktwerbung kann ebenfalls als auf berechtigten Interessen beruhend angesehen werden.

14. die Verarbeitung personenbezogener Daten zu anderen Zwecken als denen, für die sie erhoben wurden

(65) Die Verarbeitung personenbezogener Daten zu anderen Zwecken als denen, für die sie erhoben wurden, ist nur zulässig, wenn die Verarbeitung mit dem ursprünglichen Zweck der Verarbeitung vereinbar ist. Vor der Weiterverarbeitung sollte die Stellungnahme des DSB eingeholt werden.

66 Eine Weiterverarbeitung zu Archivierungs-, wissenschaftlichen, historischen Forschungs- oder statistischen Zwecken im öffentlichen Interesse ist zulässig.

TEIL V

BESCHÄFTIGUNGSBEZOGENE DATENVERARBEITUNG

15. personelle Unterlagen

(67) Im Rahmen dieses Abschnitts umfasst der Begriff "Unternehmen" auch den Arbeitgeber im Sinne des Gesetzes Nr. I aus dem Jahr 2012 über das Arbeitsgesetzbuch (nachstehend "Arbeitsgesetzbuch" genannt).

(68) Von einem Arbeitnehmer darf nur eine Aussage oder Auskunft verlangt werden, die sein Recht auf Privatsphäre nicht verletzt und für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses von Bedeutung ist.

69 Das Unternehmen muss den Arbeitnehmer über die Verarbeitung seiner personenbezogenen Daten informieren. Das Unternehmen darf Tatsachen, Daten und Meinungen über den Arbeitnehmer nur in den gesetzlich vorgesehenen Fällen oder mit Zustimmung des Arbeitnehmers an Dritte weitergeben.

70 Zur Erfüllung der sich aus dem Arbeitsverhältnis ergebenden Verpflichtungen kann das Unternehmen die personenbezogenen Daten des Arbeitnehmers an einen Datenverarbeiter übermitteln, wobei der Zweck der Datenübermittlung im Sinne des Gesetzes anzugeben ist. Der Arbeitnehmer ist hiervon im Voraus zu unterrichten.

71 Das Unternehmen darf den Arbeitnehmer nur im Zusammenhang mit seinem Verhalten im Arbeitsverhältnis kontrollieren. Die Kontrolle durch das Unternehmen und die zu ihrer Durchführung eingesetzten Mittel und Methoden dürfen nicht zu einer Verletzung der Menschenwürde führen. Das Privatleben des Arbeitnehmers darf nicht kontrolliert werden. Das Unternehmen informiert den Arbeitnehmer im Voraus über den Einsatz von technischen Mitteln, die zur Überwachung des Arbeitnehmers eingesetzt werden.

72 Die betroffene Person muss vor Beginn der Verarbeitung darüber informiert werden, dass die Verarbeitung auf der Grundlage des Arbeitsgesetzes und der berechtigten Interessen des Arbeitgebers erfolgt.

73 Das Unternehmen verarbeitet die folgenden Daten des Arbeitnehmers, um einer rechtlichen Verpflichtung nachzukommen, der es unterliegt (Artikel 6 Absatz 1 Buchstabe c DSGVO):

a) Name

b) Name bei der Geburt,,

c) Geburtsdatum,

d) den Namen der Mutter,

e) Ihre Adresse,

f) Ihre Staatsangehörigkeit,

g) Steueridentifikationsnummer,

h) Sozialversicherungsnummer,

(i) die ständige Nummer des Rentners (im Falle eines pensionierten Arbeitnehmers),

j) Nummer des Personalausweises,

k) die Nummer der amtlichen Aufenthaltsbescheinigung,

l) das Datum des Beginns und des Endes Ihrer Beschäftigung,

m) Berufsbezeichnung,

n) die Nummer des Dokuments, das Ihre allgemeine und berufliche Bildung bescheinigt,

o) die Höhe Ihres Gehalts, Daten über Ihr Gehalt und andere Leistungen,

(p) die Höhe der Schuld, die aufgrund einer rechtskräftigen Entscheidung, einer gesetzlichen Bestimmung oder einer schriftlichen Zustimmung vom Lohn des Arbeitnehmers abzuziehen ist, sowie die Berechtigung zu diesem Abzug,

q) die Art und Weise und die Gründe für die Beendigung des Arbeitsverhältnisses,

(r) eine Zusammenfassung der Eignungstests,

(s) bei Mitgliedschaft in einem privaten Rentenfonds und einem freiwilligen Versicherungsverein auf Gegenseitigkeit den Namen und die Kennnummer des Fonds sowie die Mitgliedsnummer des Arbeitnehmers,

t) bei ausländischen Arbeitnehmern die Nummer des Reisepasses, die Bezeichnung und die Nummer des Dokuments, mit dem sie ihr Recht auf Arbeit nachweisen,

u) Daten aus den Aufzeichnungen über Unfälle von Arbeitnehmern;

v) die Daten, die für die Inanspruchnahme von sozialen Diensten und gewerblichen Unterkünften erforderlich sind;

74 Das Unternehmen verarbeitet die Daten zur Wahrung der berechtigten Interessen des Arbeitgebers (Artikel 6 Absatz 1 Buchstabe f) DSGVO), zur Regelung des Arbeitsverhältnisses, zur Einhaltung der Vorschriften und zur gegenseitigen Zusammenarbeit:

a) Telefonnummer,

b) E-Mail Adresse,

c) Ihre Bankkontonummer,

d) Online-Kennung (falls vorhanden)

e) Foto,

f) einen Lebenslauf,

g) eine Bewertung der Arbeit des Arbeitnehmers,

(h) je nach Tätigkeit ein Führungszeugnis

(i) das Kamera- und Zugangskontrollsystem des Unternehmens für Sicherheits- und Eigentumsschutzzwecke und

(j) von Ortungssystemen aufgezeichnete Daten.

75 Um die Richtigkeit der Daten zu gewährleisten, muss der Arbeitnehmer jede Änderung der oben genannten Daten innerhalb von 8 Tagen schriftlich an den Leiter des Unternehmens melden.

76. die Empfänger der personenbezogenen Daten, der Geschäftsführer des Arbeitgebers, die Person, die die Befugnisse des Arbeitgebers ausübt, die Mitarbeiter des Unternehmens, die arbeitsbezogene Aufgaben erfüllen, und die Datenverarbeiter. Nur personenbezogene Daten von Arbeitnehmern in leitender Stellung dürfen an die Eigentümer des Unternehmens übermittelt werden.

(77) Nur befugte Personen haben Zugang zu den Personalakten, und es ist ein Zugangsprotokoll gemäß Anhang 6 zu führen.

78 Der Arbeitnehmer ist verpflichtet, Geschäftsgeheimnisse, von denen er im Rahmen seiner Tätigkeit erfährt, zu wahren. Darüber hinaus darf er keine Informationen, die er im Rahmen seiner Tätigkeit erlangt hat und deren Offenlegung dem Unternehmen oder einer anderen Person schaden könnte, an Unbefugte weitergeben.

79 Das Unternehmen darf Daten über Krankheit, Betriebsrats- oder Gewerkschaftszugehörigkeit nur verarbeiten, um ein Recht oder eine Pflicht aus dem Arbeitsgesetzbuch zu erfüllen.

80 Dauer der Speicherung personenbezogener Daten: 50 Jahre nach Beendigung des Beschäftigungsverhältnisses. Personenbezogene Daten müssen in Archiven aufbewahrt werden, die vor unbefugtem Zugriff und Zerstörung geschützt sind.

81 Das Unternehmen informiert den Arbeitnehmer über die Verarbeitung seiner personenbezogenen Daten und über seine persönlichen Rechte, indem es ihm bei Abschluss des Arbeitsvertrags den in Anhang 7 der vorliegenden Verordnung aufgeführten Informationsvermerk aushändigt.

16. die Verarbeitung von Daten im Zusammenhang mit Eignungstests

(82) Ein Arbeitnehmer darf nur einer Eignungsprüfung unterzogen werden, die durch eine Beschäftigungsvorschrift vorgeschrieben ist oder die für die Ausübung eines Rechts oder die Erfüllung einer Pflicht erforderlich ist, die in einer Beschäftigungsvorschrift festgelegt ist.

83 Der Arbeitgeber kann von den Arbeitnehmern verlangen, dass sie sowohl vor der Begründung des Arbeitsverhältnisses als auch während des Arbeitsverhältnisses Testbögen zur Überprüfung der Arbeitsfähigkeit und -bereitschaft ausfüllen.

84. psychologische oder persönlichkeitsbezogene Testbögen, die eindeutig auf das Arbeitsverhältnis bezogen sind, können von einer größeren Gruppe von Arbeitnehmern ausgefüllt werden, um Arbeitsabläufe effizienter durchzuführen und zu organisieren, jedoch nur, wenn die aus der Analyse hervorgehenden Daten nicht mit einzelnen Arbeitnehmern in Verbindung gebracht werden können, d. h. die Daten werden anonym verarbeitet.

85 Vor der Beurteilung müssen die Beschäftigten außerdem ausführlich über die zu beurteilenden Fähigkeiten und Fertigkeiten, die Mittel und Methoden der Beurteilung, die Auswirkungen der Beurteilung auf ihre Rechte, die Möglichkeit des persönlichen Eingreifens und die Frage, ob automatisierte Entscheidungsfindung und Profiling eingesetzt werden, informiert werden. Ist die Durchführung der Beurteilung gesetzlich vorgeschrieben, müssen die Mitarbeiter auch über die gesetzlichen Bestimmungen informiert werden. Ein Muster für einen Datenschutzhinweis ist in Anhang 8 zu dieser Richtlinie enthalten.

86 Im Anschluss an die Unterrichtung kann der Arbeitgeber von den Arbeitnehmern Testbögen ausfüllen lassen, um deren Eignung und Arbeitsbereitschaft sowohl vor der Begründung des Arbeitsverhältnisses als auch während des Arbeitsverhältnisses zu messen. Das Ausfüllen der Testbögen darf nicht dazu benutzt werden, die Arbeitnehmer zu schikanieren oder ihre Rechte zu verletzen.

Um Arbeitsprozesse effizienter durchführen und organisieren zu können, kann eine für die psychologische Forschung oder die Erforschung von Persönlichkeitsmerkmalen geeignete Testform nur dann mit einer großen Gruppe von Arbeitnehmern durchgeführt werden, wenn die bei der Auswertung gewonnenen Daten nicht mit einzelnen Arbeitnehmern in Verbindung gebracht werden können, d.h. die Daten anonymisiert verarbeitet werden.

88 Der Umfang der personenbezogenen Daten, die verarbeitet werden können, ist die Tatsache der Eignung für die Stelle und die Festlegung der erforderlichen Bedingungen. Rechtsgrundlage für die Verarbeitung: berechtigtes Interesse des Arbeitgebers. Zweck der

Verarbeitung personenbezogener Daten für die Begründung und Aufrechterhaltung eines Beschäftigungsverhältnisses, die Besetzung einer Stelle

89 Die Ergebnisse der Untersuchung dürfen nur den betroffenen Arbeitnehmern oder dem Untersuchungsbeauftragten mitgeteilt werden, der zur Vertraulichkeit verpflichtet ist. Der Arbeitgeber darf nur darüber unterrichtet werden, ob die untersuchte Person für den Arbeitsplatz geeignet ist oder nicht und welche Bedingungen dafür zu schaffen sind. Die Einzelheiten der Untersuchung und ihre vollständige Dokumentation dürfen dem Arbeitgeber nicht mitgeteilt werden.

90 Personenbezogene Daten dürfen 50 Jahre lang nach Beendigung des Beschäftigungsverhältnisses verarbeitet werden. Tests und Beurteilungen von Mitarbeitern sind getrennt von den Personalakten aufzubewahren und unter Verschluss zu halten.

17. die Verwaltung von Lebensläufen

(91) Um sicherzustellen, dass die Datenschutzrechte des Einreichers eines Lebenslaufs, der nicht aus einer Ausschreibung resultiert, nicht verletzt werden, sollte auf der Website des Unternehmens unter dem Link "Kontakt" ein Hinweis auf die Verarbeitung und Speicherung von Lebensläufen platziert werden, in dem darauf hingewiesen wird, dass die betroffene Person dem eingereichten Lebenslauf eine Einverständniserklärung für die Verarbeitung ihres Lebenslaufs für einen Zeitraum von drei Monaten beifügen sollte. Enthält die eingegangene Erklärung diese Zustimmung nicht, ist das Unternehmen lediglich berechtigt zu prüfen, ob es eine dem Bewerbungsdossier entsprechende Stelle zu besetzen hat, und wenn dies nicht der Fall ist, muss das Dossier an den Einsender zurückgeschickt oder vernichtet werden.

92 In der Stellenausschreibung ist darauf hinzuweisen, dass die Aufbewahrungsfrist für Lebensläufe drei Monate ab dem Tag des Ablaufs der Frist für die Einreichung der entsprechenden Bewerbung beträgt bzw. drei Monate ab dem Tag der Einreichung der Bewerbung, wenn diese unabhängig von der Bewerbung eingegangen ist. Die Lebensläufe von nicht eingestellten Personen können aufbewahrt werden, um eine Stelle zu besetzen, die zwar eingestellt wurde, aber während der Probezeit frei wird.

(93) Nach Ablauf der Datenaufbewahrungsfrist oder nach Widerruf der Einwilligung der betroffenen Person werden die Bewerbungsunterlagen vernichtet oder auf ausdrücklichen Wunsch des Antragstellers an diesen zurückgegeben. Über die Vernichtung der Daten, die keine personenbezogenen Daten enthalten, wird ein Protokoll gemäß Anhang 9 erstellt.

94 Umfang der verarbeiteten personenbezogenen Daten, Name, Geburtsdatum und -ort, Name der Mutter, Anschrift, Qualifikationen, Foto, Telefonnummer, E-Mail-Adresse, Beurteilung des früheren Arbeitgebers (falls vorhanden).

95 Der Zweck der Verarbeitung personenbezogener Daten ist die Auswahl des richtigen Personals. Die betroffene Person muss informiert werden, wenn der Arbeitgeber sie nicht für die Stelle ausgewählt hat.

96 Rechtsgrundlage für die Verarbeitung, Einwilligung der betroffenen Person.

97 Lebensläufe können von leitenden Angestellten bearbeitet werden, die befugt sind, Arbeitgeberrechte im Unternehmen auszuüben, und die Personalaufgaben wahrnehmen.

(98) Macht sich der Unternehmensvertreter während des Gesprächs Notizen, so ist die Zustimmung des Betroffenen im Voraus einzuholen, und der Betroffene muss am Ende des Gesprächs Zugang zu den Notizen erhalten und sich dazu äußern können. Am Ende des Gesprächs unterschreibt der Betroffene den Vermerk, wenn er mit dessen Inhalt einverstanden ist; verweigert er seine Unterschrift, wird der Vermerk vernichtet.

99 Das Unternehmen ist nicht berechtigt, frühere Arbeitgeber im Zusammenhang mit der Bewerbung zu kontaktieren.

100 Das Unternehmen kann die öffentlich geposteten Daten des Bewerbers auf der Website des sozialen Netzwerks überprüfen (aber nicht speichern), worauf es bei der Bewerbung und auf der Website hinweist. Das Unternehmen darf keine Aktivitäten im Zusammenhang mit einer geschlossenen Gruppe auf der Social-Networking-Website des Bewerbers überwachen.

101 Das Unternehmen schaltet keine anonymen Stellenanzeigen.

In § 10 (1) (e) des Regierungsdekrets 118/2001 (VI. 30.) ist festgelegt, welche Daten im Rahmen einer privaten Beschäftigung nicht verarbeitet werden dürfen. Das Gesetz verbietet die Verarbeitung personenbezogener Daten, die nicht für die Beurteilung der Eignung des Arbeitssuchenden erforderlich sind oder die nicht in direktem Zusammenhang mit der gesuchten Stelle stehen.

103 Für jeden Teil der Bewerbung kann ein amtliches Führungszeugnis verlangt werden.

18. die Datenverarbeitung im Zusammenhang mit der Überwachung der elektronischen Post

104 Das Unternehmen stellt dem Arbeitnehmer ein E-Mail-Konto zur Verfügung, dessen E-Mail-Adresse und Konto der Arbeitnehmer im Rahmen seiner beruflichen Tätigkeit für die

Kommunikation untereinander oder für die Korrespondenz mit Kunden, anderen Personen und Organisationen im Namen des Arbeitgebers nutzen kann. Den Arbeitnehmern ist es nicht gestattet, das elektronische Postsystem für private Zwecke zu nutzen oder persönliche Korrespondenz über das Konto zu führen, woran das Unternehmen seine Arbeitnehmer alle sechs Monate erinnert.

105 Die Rechtsgrundlage für die Kontrolle ist das berechtigte Interesse und der Zweck des Arbeitgebers, die Einhaltung der Pflichten des Arbeitsverhältnisses zu überprüfen und die ordnungsgemäße Ausführung der Arbeit sicherzustellen.

106 Der Verwalter sorgt für die IT-Sicherheit des elektronischen Postsystems des Unternehmens.

107 Bei der Nutzung des Systems der elektronischen Post muss der betreffende Mitarbeiter bei der Angabe von Empfängern, der Verwendung von Geheimkopien und dem Anhängen von Dokumenten die erforderliche Sorgfalt walten lassen. Es sollte darauf geachtet werden, dass die mit den Empfängern und der Person, die Kopien erhält, verknüpfte E-Mail-Adresse ebenfalls personenbezogene Daten sind.

108. im elektronischen Schriftverkehr sollten Anstrengungen unternommen werden, personenbezogene Daten zu verschlüsseln. Entwürfe von Dokumenten sollten ohne Angabe personenbezogener Daten zur Einsichtnahme übermittelt werden.

109 Die Nutzung des Mailsystems am Arbeitsplatz ist nur auf Geräten am Arbeitsplatz erlaubt.

110 Der Arbeitgeber hat das Recht, den Inhalt und die Nutzung des E-Mail-Kontos regelmäßig - alle 3 Monate - zu überprüfen. Zweck der Überwachung ist es, die Einhaltung der Bestimmungen des Arbeitgebers über die Nutzung des E-Mail-Kontos zu überprüfen und die Erfüllung der Pflichten des Arbeitnehmers zu kontrollieren, wobei die Rechtsgrundlage das berechtigte Interesse des Arbeitgebers ist.

111 Der Leiter des Arbeitgebers oder die Person, die die Rechte des Arbeitgebers ausübt, ist berechtigt, die Kontrolle und die Datenverarbeitung durchzuführen.

112. wenn möglich, dafür sorgen, dass der Arbeitnehmer bei der Inspektion anwesend ist, und in seiner Abwesenheit die Beobachtungen in Anwesenheit von zwei Personen aufzeichnen

113 Vor der Kontrolle ist der Arbeitnehmer über das Interesse des Arbeitgebers an der Kontrolle, das Interesse des Arbeitgebers an der Kontrolle, die Personen, die die Kontrolle durchführen dürfen, - die Regeln, nach denen die Kontrolle stattfinden kann, und das einzuhaltende Verfahren, - die Rechte und Rechtsbehelfe des Arbeitnehmers im Zusammenhang mit den Ergebnissen der Kontrolle zu informieren.

114 Bei der Überprüfung sollte der Grundsatz der Progression angewandt werden, so dass in erster Linie aus dem Titel und dem Betreff des Schreibens geschlossen werden kann, dass es sich um ein Schreiben im Zusammenhang mit den beruflichen Aufgaben des Arbeitnehmers und nicht um ein persönliches Schreiben handelt. Der Inhalt von nicht-persönlichen E-Mails kann vom Unternehmen uneingeschränkt geprüft werden.

115 Kann festgestellt werden, dass der Arbeitnehmer das System der elektronischen Post für persönliche Zwecke genutzt hat, sollte er aufgefordert werden, die personenbezogenen Daten unverzüglich zu löschen. Bei Abwesenheit oder Nichtmitarbeit des Arbeitnehmers werden die personenbezogenen Daten nach Überprüfung durch den Arbeitgeber gelöscht.

116. 56 des Arbeitsvertrags.

(117) Die Arbeitnehmer können die im Abschnitt dieses Kodex über die Rechte der betroffenen Personen dargelegten Rechte in Bezug auf die Verarbeitung von Daten, die eine Überwachung der elektronischen Post beinhalten, ausüben.

118 Vor Beendigung des Arbeitsverhältnisses hat der Arbeitnehmer dafür zu sorgen, dass der private Schriftverkehr gelöscht wird. Nach Beendigung des Arbeitsverhältnisses vernichtet das Unternehmen die im System der elektronischen Post gespeicherten personenbezogenen Daten.

119 Das Unternehmen erhält vom Softwareentwickler die Ergebnisse der Folgenabschätzung zur Einhaltung der DSGVO für das verwendete Arbeitsplatz-Mailsystem.

120 Ein Mitarbeiter, der eine Unregelmäßigkeit im Betrieb des Mailsystems feststellt oder Kenntnis von personenbezogenen Daten erhält, zu denen er nicht berechtigt ist, muss dies unverzüglich dem Verwalter und dem Leiter des Unternehmens melden.

19. die Datenverarbeitung im Zusammenhang mit der Kontrolle von IT-Tools

121 Das Unternehmen legt hiermit fest, dass die vom Unternehmen zur Verfügung gestellten Computer oder elektronischen Geräte, insbesondere Computer, Laptops und Tablets, vom

Arbeitnehmer nur zu Arbeitszwecken genutzt werden dürfen und das Unternehmen die private Nutzung solcher Geräte untersagt und der Arbeitnehmer keine persönlichen Daten oder Korrespondenz auf solchen Geräten verarbeiten oder speichern darf.

(122) Es muss sichergestellt werden, dass die elektronischen Geräte regelmäßig - alle sechs Monate - auf einem Server gesichert werden, und die betroffenen Personen müssen aufgefordert werden, alle auf den Datenträgern vorhandenen personenbezogenen Daten zu löschen.

123 Andere Geräte als die vom Unternehmen zur Verfügung gestellten mobilen Datenträger dürfen nicht an die IT-Einrichtungen des Unternehmens angeschlossen werden, und es muss durch Passwortschutzkontrollen sichergestellt werden, dass die Nutzung fremder Geräte ausgeschlossen ist.

124 Der Verwalter des Unternehmens veranlasst die Reparatur des IT-Geräts, und wenn er nicht in der Lage ist, es zu reparieren, muss er zum Zeitpunkt der Reparatur anwesend sein, um einen unbefugten Zugriff auf personenbezogene Daten auf dem Speichermedium des IT-Geräts zu verhindern. Bei der Reparatur durch einen Dritten kann der IT-Administrator abwesend sein, wenn er keinen Datenträger (winchester) zur Verfügung stellt oder der Dritte bescheinigt, dass seine Tätigkeit mit der DSGVO übereinstimmt und eine Vertraulichkeitserklärung abgibt.

125 Die physische Zerstörung des Speichermediums muss sichergestellt werden, bevor die IT-Ausrüstung verschrottet oder verkauft wird.

126 Vor der Beendigung des Arbeitsverhältnisses hat der Arbeitnehmer dafür zu sorgen, dass alle privaten Daten auf dem IT-Gerät gelöscht werden. Nach Beendigung des Arbeitsverhältnisses hat das Unternehmen die auf dem IT-Gerät gespeicherten personenbezogenen Daten zu vernichten.

(127) Der Arbeitgeber darf die auf den IT-Geräten gespeicherten Daten kontrollieren. Im Übrigen gelten für die Kontrolle der Informatikmittel durch den Arbeitgeber und die damit verbundenen Rechtsfolgen die Bestimmungen des Titels 18.

128 Die Beschäftigten müssen den Verlust ihrer IT-Ausrüstung innerhalb von 24 Stunden dem Leiter des Unternehmens melden und dabei die ungefähre Menge und Art der auf der Ausrüstung befindlichen personenbezogenen Daten angeben.

129 Telearbeit kann unter Verwendung der vom Unternehmen zur Verfügung gestellten IT-Ausrüstung genehmigt werden. Im Falle von Telearbeit muss der Arbeitnehmer über die Vorschriften zur Kontrolle durch das Unternehmen und die Beschränkungen bei der Nutzung

der IT-Ausrüstung gemäß Titel 18 und diesem Titel sowie über die Abteilung, in der der Arbeitnehmer arbeitet, informiert werden.

(130) Der Verwalter sorgt für den Schutz der IT-Geräte und trifft geeignete Maßnahmen, um sicherzustellen, dass bei Verlust des Geräts kein Zugriff auf die gespeicherten personenbezogenen Daten möglich ist.

20. die Datenverarbeitung zum Zwecke der Überwachung der Internetnutzung am Arbeitsplatz

131 Die Beschäftigten dürfen nur Websites aufrufen, die mit ihren beruflichen Aufgaben in Zusammenhang stehen, und der Arbeitgeber verbietet die Nutzung des Internets für private Zwecke am Arbeitsplatz.

132 Im Internet verfügbare Software darf auf den IT-Geräten des Unternehmens nur mit Genehmigung des Administrators installiert werden. Der Administrator genehmigt die Installation von Software nach Angabe eines Administrator-Benutzernamens und eines Passworts, entweder persönlich oder per Fernzugriff. Die Verwendung von nicht genehmigter Software, die aus externen Quellen bezogen oder von externen Quellen heruntergeladen wurde, ist verboten!

133 Der Besuch von Websites, die das Herunterladen von Dateien, Spiele, Chats oder sexuelle Dienstleistungen anbieten, ist streng verboten.

134 Das Unternehmen ist der Inhaber der Internetregistrierungen, die im Namen des Unternehmens als berufsbezogene Aufgabe durchgeführt werden, und die Registrierung muss unter Verwendung einer Kennung und eines Passworts erfolgen, die auf das Unternehmen verweisen. Für die Registrierung müssen auch die persönlichen Daten angegeben werden, und das Unternehmen veranlasst die Löschung der persönlichen Daten bei Beendigung des Beschäftigungsverhältnisses.

135 Das Unternehmen kann die Internetnutzung des Arbeitnehmers am Arbeitsplatz gemäß den Bestimmungen des Titels 18 überwachen und die darin vorgesehenen gesetzlichen Sanktionen anwenden.

21. die Datenverarbeitung im Zusammenhang mit der Kontrolle der Nutzung von Firmenhandys

136 Das Unternehmen erlaubt keine private Nutzung des Firmenhandys, es darf nur für arbeitsbezogene Zwecke verwendet werden, und das Unternehmen kann alle ausgehenden Nummern und Daten sowie die auf dem Handy gespeicherten Daten überwachen.

137 Arbeitnehmer müssen dem Unternehmen melden, wenn sie ihr Firmenhandy für private Zwecke nutzen. Der Arbeitgeber hat das Recht, den Arbeitnehmer zu melden, wenn die Telefonrechnung des Arbeitnehmers mehr als 50 % über dem Durchschnitt der anderen Arbeitnehmer in der gleichen Position liegt. In einem solchen Fall wird das Unternehmen vom Telefondienstanbieter Einzelheiten zu den Gesprächsaufzeichnungen anfordern und den Arbeitnehmer auffordern, die zu privaten Zwecken angerufenen Nummern unkenntlich zu machen. Das Unternehmen kann vom Arbeitnehmer verlangen, dass er die Kosten für private Anrufe übernimmt.

138 Der Arbeitnehmer hat dafür zu sorgen, dass alle privaten Telefonnummern vor Beendigung seines Arbeitsverhältnisses gelöscht werden. Nach Beendigung des Arbeitsverhältnisses vernichtet das Unternehmen die auf dem Mobiltelefon gespeicherten personenbezogenen Daten.

139 Die Mitarbeiter müssen den Unternehmensleiter innerhalb von 24 Stunden informieren, wenn sie ihr Firmenhandy verlieren.

Die Mobiltelefone der Unternehmen müssen mit einem Programm ausgestattet sein, das es ermöglicht, den Bildschirm zu sperren und die auf dem Telefon und der SIM-Karte gespeicherten Daten zu löschen, falls eine unbefugte Person auf die auf dem Telefon gespeicherten persönlichen Daten zugreifen möchte.

(141) Für die Kontrolle und ihre Folgen gelten die Bestimmungen von Titel 18.

22. die Verarbeitung von Daten im Zusammenhang mit der Nutzung des Navigationssystems

Rechtsgrundlage für den Einsatz eines Navigationssystems (GPS) ist das berechtigte Interesse des Arbeitgebers, dessen Zweck die effiziente Organisation von Arbeitsabläufen, die Logistik, die Wahrung der Geschäftsinteressen des Arbeitgebers und der Schutz von Leib und Leben der Arbeitnehmer, des Fahrzeugs und der transportierten Ausrüstung ist.

143 Die verarbeiteten Daten sind das Kennzeichen des Fahrzeugs, die zurückgelegte Strecke, die Entfernung, der Standort und die Nutzungszeit des Fahrzeugs.

(144) Die Kontrolle darf nur während der Arbeitszeit durchgeführt werden, und der geografische Standort der Arbeitnehmer darf nicht außerhalb der Arbeitszeit kontrolliert

werden. Im Übrigen gelten für die Kontrolle und ihre Folgen die Bestimmungen des Titels 19 mit der Ausnahme, dass der Arbeitgeber berechtigt ist, dem Arbeitnehmer mitzuteilen, wenn die Entfernungen zwischen den im Fahrtenblatt angegebenen Orten um mehr als 20 % von der Routenplanung abweichen; in diesem Fall kann der Arbeitnehmer zur Erstattung der Kosten verpflichtet werden.

145 Das Unternehmen wird die Ergebnisse der Folgenabschätzung zur Einhaltung der DSGVO für das verwendete Navigationssystem einholen.

23. die Verarbeitung von Daten im Zusammenhang mit der Videoüberwachung am Arbeitsplatz

146 Das Unternehmen setzt in seinem Hauptsitz und in den für Kunden zugänglichen Räumlichkeiten ein elektronisches Überwachungssystem zum Schutz von Menschenleben, körperlicher Unversehrtheit und Eigentum ein, das auch die Aufzeichnung und Speicherung von Bildern ermöglicht, auf deren Grundlage das von der Kamera aufgezeichnete Verhalten der betroffenen Person als personenbezogene Daten betrachtet werden kann. Im Falle des Schutzes eines bestimmten Objekts muss die Kamera direkt und ausschließlich auf das zu schützende Objekt gerichtet sein.

147 Die Rechtsgrundlage für die Verarbeitung sind die berechtigten Interessen des Arbeitgebers und des Opfers an den Kameraaufzeichnungen.

(148) Vor dem Betreten des überwachten Bereichs ist an einer gut sichtbaren und lesbaren Stelle ein Hinweis anzubringen, der die betroffenen Personen über den Einsatz des Überwachungssystems in diesem Bereich informiert. Die Informationen sind für jede Kamera bereitzustellen. Ein Muster für die Informationen ist in Anhang 10 enthalten.

(149) Ein elektronisches Überwachungssystem oder eine andere technische Kontrollvorrichtung darf nicht an Orten eingesetzt werden, an denen eine solche Überwachung die Menschenwürde verletzen kann, insbesondere in Umkleideräumen, Toiletten, Waschräumen, Räumen für medizinische oder psychologische Untersuchungen, einschließlich Warteräumen in Untersuchungsräumen. Das Überwachungssystem darf nicht auf öffentliche Bereiche gerichtet sein.

150 Im Rahmen der technischen Überwachung darf keine Kamera zur Beobachtung der Arbeit oder des Verhaltens am Arbeitsplatz in Räumen, in denen ständig gearbeitet wird, sowie in Räumen, die während der Arbeitszeit zum Ausruhen genutzt werden, in ausgewiesenen Raucherbereichen oder in Bereitschaftsräumen aufgestellt werden.

Ausgenommen hiervon sind Arbeitsplätze, an denen das Leben und die körperliche Unversehrtheit von Arbeitnehmern gefährdet sein können, z. B. wenn eine Kamera in einem Arbeitsraum oder in einem Objekt oder Raum mit anderen Gefahrenquellen betrieben werden kann.

152 Aufgezeichnetes Bildmaterial darf höchstens 3 (drei) Arbeitstage lang aufbewahrt werden, wenn es nicht verwendet wird. Eine Verwendung gilt als erfolgt, wenn die aufgezeichneten Bilder und sonstigen personenbezogenen Daten als Beweismittel in einem gerichtlichen oder sonstigen behördlichen Verfahren verwendet werden sollen. Eine Person, deren Recht oder berechtigtes Interesse durch die Aufzeichnung der Daten aus einer Bildaufzeichnung beeinträchtigt wird, kann innerhalb von drei Arbeitstagen nach der Aufzeichnung der Bildaufzeichnung verlangen, dass die Daten von dem für die Verarbeitung Verantwortlichen nicht vernichtet oder gelöscht werden, indem sie ihr Recht oder berechtigtes Interesse nachweist

(153) In den Räumlichkeiten, in denen Waren von bedeutendem Wert gelagert werden, insbesondere in Garagen, Lagern für andere Waren von bedeutendem Wert und in den Gängen, die zu ihnen führen, kann eine Kamera installiert und betrieben werden, doch muss der Betrieb der Kamera deutlich angezeigt und den betroffenen Personen deutlich mitgeteilt werden.

154 Darf sich niemand auf dem Betriebsgelände aufhalten, insbesondere außerhalb der Arbeitszeiten oder an Feiertagen, kann der gesamte Arbeitsplatz (z. B. Umkleideräume, Toiletten, Pausenräume) überwacht werden.

155 Die Geräte, die das von den Kameras aufgenommene Bild übertragen, müssen so angebracht sein, dass sie nur von der Person eingesehen werden können, deren Aufgabe es ist, das von der Kamera übertragene Bild zu überwachen. Das Betriebspersonal, der Betriebsleiter und sein Stellvertreter sowie der Leiter des überwachten Bereichs sind befugt, die aufgezeichneten Daten zum Zwecke der Feststellung von Verstößen und der Überprüfung der Funktionsweise des Systems einzusehen.

(156) Die Überwachung und Überprüfung gespeicherter Bilder darf nur zum Zweck der Aufdeckung von Rechtsverletzungen und der Einleitung der erforderlichen Maßnahmen zu deren Unterbindung erfolgen.

(157) Das von den Kameras übermittelte Bild darf nur von der Datenspeichereinheit aufgezeichnet werden.

158. der Datenspeicher muss unter Verschluss gehalten werden. Beim Zugriff auf die gespeicherten Bilder muss die Identität des für die Verarbeitung Verantwortlichen identifizierbar bleiben. Die Überprüfung und Sicherung der Bildaufzeichnungen muss dokumentiert werden.

(159) Der Zugang zu gespeicherten Bildaufzeichnungen wird unmittelbar nach Wegfall des Grundes für die Beendigung des Rechts beendet. Das Kontrollgerät muss das Betriebssystem und die gespeicherten Bilder von einer separaten Festplatte aus betreiben. Eine gesonderte Sicherung der Aufzeichnungen ist nicht vorzunehmen.

160 Nach der Feststellung einer rechtswidrigen Handlung wird die Aufnahme der Handlung und die Einleitung des erforderlichen Verfahrens veranlasst und die verfolgungsberechtigte Stelle von der Aufnahme der Handlung unterrichtet.

161 Vor der Übermittlung der gespeicherten Bilder muss sichergestellt werden, dass keine nicht veröffentlichungsfähigen Daten enthalten sind und die Persönlichkeitsrechte Dritter nicht verletzt werden. Nicht veröffentlichungspflichtige Daten müssen anonymisiert werden (z. B. Registrierungsnummern, Dritte).

162 Das Unternehmen erhält die Ergebnisse der Folgenabschätzung zur Vereinbarkeit des verwendeten Überwachungssystems mit der Datenschutz-Grundverordnung.

24. die Verarbeitung von Daten über Studienverträge

(163) Das Unternehmen kann mit dem Arbeitnehmer einen Studienvertrag abschließen; bevor die Verarbeitung beginnt, muss offengelegt werden, dass die Verarbeitung auf dem Vertrag beruht; dies kann im Vertrag offengelegt werden.

164 Die Rechtsgrundlage für die Verarbeitung ist der Vertrag, die Dauer der Verarbeitung beträgt 50 Jahre.

(165) Die personenbezogenen Daten der betroffenen Person können an die Bildungseinrichtung, die die Ausbildung durchführt, als gemeinsam für die Verarbeitung Verantwortlicher übermittelt werden; dies muss im Vertrag angegeben werden.

166 Der Wortlaut der Mitteilung über den Vertrag mit dem Arbeitnehmer ist in Anhang 11 wiedergegeben.

167 Die personenbezogenen Daten können von Mitarbeitern und Datenverarbeitern des Unternehmens, die Personalfunktionen wahrnehmen, verarbeitet werden.

(168) Beim Abschluss eines Studienvertrags sind die Bestimmungen des § 229 Abs. 1 des Arbeitsgesetzbuchs und andere Bestimmungen des Gesetzes zu berücksichtigen.

TEIL VII

EINWILLIGUNG ALS RECHTSGRUNDLAGE FÜR DIE VERARBEITUNG

25. die Verarbeitung von Daten über das Surfen auf der Website (Cookies)

Ein Cookie ist ein Datenelement, das die besuchte Website an den Browser des Besuchers sendet, damit dieser seine Inhalte speichern und später laden kann.

170 Die Rechtsgrundlage für die Verarbeitung ist die Einwilligung der betroffenen Person.

171 Die Daten dürfen auf dem IT-Gerät des Nutzers gespeichert werden, oder der Zugriff auf die dort gespeicherten Daten darf nur auf der Grundlage der eindeutigen und vollständigen Zustimmung des Nutzers gewährt werden, einschließlich des Zwecks der Datenverarbeitung (gemäß Artikel 155 (4) des Gesetzes C von 2003).

172 Beim Besuch der Website des Unternehmens sollte eine kurze Zusammenfassung über die Verwendung von Cookies gegeben werden, und der vollständige Text des Hinweises sollte über einen Link gemäß Anhang 12 zugänglich gemacht werden. Mit dem Informationshinweis stellt das Unternehmen sicher, dass der Besucher vor und jederzeit während der Nutzung der Dienste der Website darüber informiert werden kann, zu welchen Zwecken das Unternehmen welche Arten von Daten verarbeitet, einschließlich Daten, die nicht direkt mit dem Nutzer in Verbindung gebracht werden können.

Gemäß Artikel 13/A (3) des Gesetzes CVIII von 2001 über bestimmte Aspekte der Dienste des elektronischen Geschäftsverkehrs und der Informationsgesellschaft (E-Commerce-Gesetz) kann der Diensteanbieter personenbezogene Daten verarbeiten, die für die Erbringung des Dienstes technisch unerlässlich sind. Der Diensteanbieter muss unter sonst gleichen Bedingungen die verwendeten Mittel so wählen und einsetzen, dass personenbezogene Daten nur in dem Umfang und für die Dauer verarbeitet werden, die für die Erbringung des Dienstes und für die Erfüllung der anderen in diesem Gesetz genannten Zwecke erforderlich sind.

26. auf der Website registrieren

174 Die natürliche Person, die sich auf der Website anmeldet, kann ihre Zustimmung zur Verarbeitung ihrer personenbezogenen Daten geben, indem sie das entsprechende leere Kästchen (Checkbox) ankreuzt.

175. der Umfang der verarbeiteten personenbezogenen Daten: Name (Nachname, Vorname), Anschrift, Telefonnummer, E-Mail-Adresse, Online-Kennung, Name und Anschrift der natürlichen Person für Rechnungsstellung und Postversand. Die Angabe eines Benutzernamens oder eines Passworts ist nicht erforderlich und darf auch nicht in einer Antwortnachricht verlangt werden.

176 Nach der Registrierung auf der Website muss eine Bestätigungsnachricht an die von der registrierenden Person angegebenen elektronischen Kontaktdaten gesendet werden, um sicherzustellen, dass das Unternehmen sich vergewissert hat, dass die betroffene Person sich mit ihren eigenen Daten auf der Website registriert hat. Solange die Bestätigung nicht vorliegt, können die Daten nicht verarbeitet werden, und wenn keine Bestätigung eingeht, werden die Daten nach einem Monat gelöscht.

177 Die Rechtsgrundlage für die Verarbeitung ist die Einwilligung der betroffenen Person, der Zweck der Verarbeitung:

a) die Bereitstellung von Dienstleistungen auf der Website;

b) Kontaktaufnahme mit Ihnen (elektronisch, telefonisch, per SMS und per Post);

c) Informationen über die Produkte, Dienstleistungen, Geschäftsbedingungen und Werbeaktionen des Unternehmens;

d) das Senden einer Werbebotschaft;

e) Analyse der Nutzung der Website.

Die personenbezogenen Daten können von den Mitarbeitern des Unternehmens, die Aufgaben im Zusammenhang mit der Kundenbetreuung und Marketingaktivitäten wahrnehmen, sowie von den Mitarbeitern des IT-Dienstleisters des Unternehmens als Datenverarbeiter zum Zwecke der Bereitstellung des Hosting-Dienstes verarbeitet werden.

179 Personenbezogene Daten können gespeichert werden, bis die betroffene Person ihre Einwilligung widerruft.

27. die Verarbeitung der bei Veranstaltungen aufgenommenen Bilder

180 Im Falle der Organisation einer beruflichen Veranstaltung kann das Unternehmen eine Video- oder audiovisuelle Aufzeichnung der Veranstaltung anfertigen. Rechtsgrundlage für die Verarbeitung: Einwilligung der betroffenen Person.

181 Im Zusammenhang mit der Teilnahme an Bild- oder Bild- und Tonaufnahmen darf die Verarbeitung des Bildes als personenbezogene Daten nur mit vorheriger Einwilligung der betroffenen Person erfolgen, es sei denn, sie ist gesetzlich zugelassen. Die Einwilligung der betroffenen Person ist durch Ausfüllen der Erklärung in Anhang 4 einzuholen, es sei denn, die Aufnahme erfolgt:

a) ist eine Aufnahme, die während eines öffentlichen Auftritts gemacht wurde,

b) eine Massenaufzeichnung darstellt; oder

(c) wenn die Aufzeichnung des Arbeitnehmers im Rahmen einer technischen Kontrolle erfolgt, gemäß der Bestimmung über die Videoüberwachung.

182 Die Unterzeichnung der Einwilligungserklärung ist freiwillig. Personen, die nicht in die Aufzeichnungen aufgenommen werden wollen, müssen sich unter Angabe ihres Namens und ihrer Stellung registrieren lassen, um dieses Recht wahrnehmen zu können.

(183) Die Einverständniserklärungen werden von der für die Organisation der Veranstaltung benannten Person eingesammelt, die Aufzeichnungen werden aufbewahrt und weggeschlossen. Die erfassten Namen sind nur den für die Verarbeitung der Aufzeichnungen verantwortlichen Personen und dem Datenschutzbeauftragten bekannt.

184 Bei Bild- und Tonaufnahmen auf der Veranstaltung muss der für die Veranstaltung Verantwortliche die betroffenen Personen vor Beginn der Veranstaltung darauf hinweisen, dass sie den anwesenden Fotografen informieren müssen, wenn sie mit der Aufnahme von Bildern, einschließlich Aufnahmen von Menschenmengen und öffentlichen Auftritten, nicht einverstanden sind.

185 Bei Veranstaltungen, bei denen ein Teilnahme- oder Anmeldeformular verwendet wird, sollte der Datenschutzhinweis an einer gut sichtbaren Stelle angebracht werden, und es sollte ein gesonderter Abschnitt für die Zustimmung zur Datenverarbeitung auf dem Teilnahme- oder Anmeldeformular vorgesehen werden.

186 Der Zweck der Verarbeitung personenbezogener Daten besteht darin, den sozialen Zusammenhalt zu stärken und ein gutes Arbeitsklima zu schaffen.

187 Personenbezogene Daten können gespeichert werden, bis die Einwilligung widerrufen wird.

TEIL VII

VERTRAG ALS RECHTSGRUNDLAGE FÜR DIE VERARBEITUNG

28 Verarbeitung von Daten der Vertragsparteien

188. Das Unternehmen verarbeitet zum Zwecke des Abschlusses, der Durchführung, der Beendigung oder der Gewährung eines Vertragsrabatts den Namen, den Namen der mit ihm als Käufer oder Lieferant kontrahierten natürlichen Person, den Namen der natürlichen Person, den Geburtsnamen, das Geburtsdatum, den Namen der Mutter, die Adresse, die Steueridentifikationsnummer, die Steuernummer, die Nummer des Selbständigen, den Personalausweis des Selbständigen, die Nummer des Personalausweises, Anschrift, Anschrift des Geschäftssitzes, Anschrift der Niederlassung, Telefonnummer, E-Mail-Adresse, Website-Adresse, Bankkontonummer, Kundennummer (Kundennummer, Auftragsnummer), Online-Kennung (Kundenliste, Lieferantenliste, Vielkäuferliste), Diese Verarbeitung wird auch dann als rechtmäßig angesehen, wenn die Verarbeitung erforderlich ist, um auf Antrag der betroffenen Person vor Abschluss eines Vertrags Maßnahmen zu ergreifen.

189 Personenbezogene Daten können von den Mitarbeitern des Unternehmens, die kaufmännische, Kundendienst-, Buchhaltungs- und Steueraufgaben wahrnehmen, sowie von den Datenverarbeitern verarbeitet werden.

190 Dauer der Verarbeitung personenbezogener Daten: 8 Jahre nach Beendigung des Vertrags zum Zweck der Buchführung.

191 Die betroffene natürliche Person muss vor Beginn der Verarbeitung darüber informiert werden, dass die Verarbeitung auf einem Vertrag beruht, der im Vertrag enthalten sein kann. Die betroffene Person kann ihre personenbezogenen Daten an einen Auftragsverarbeiter übermitteln lassen, der im Vertrag darüber informiert werden muss. Der Wortlaut des Informationsvermerks über die Verarbeitung des Vertrags mit der natürlichen Person ist in Anhang 11 wiedergegeben.

29 Kontaktdaten der Kontaktpersonen der Partner der juristischen Person

192 Das Unternehmen verarbeitet den Namen, die Anschrift, die Telefonnummer, die E-Mail-Adresse und die Online-Kennung der betroffenen natürlichen Person auf der Rechtsgrundlage der Vertragserfüllung und der damit verbundenen Interessen des Arbeitgebers.

Im Vertrag erklären die für die Verarbeitung Verantwortlichen in Anhang 11, dass sie eine Person als Ansprechpartner benennen, die für die Erfüllung ihrer Aufgaben relevant ist und die darüber informiert wurde, dass sie von anderen für die Verarbeitung Verantwortlichen im Zusammenhang mit den Tätigkeiten des für die Verarbeitung Verantwortlichen mit vom Arbeitgeber bereitgestellten Mitteln während der Arbeitszeiten kontaktiert werden kann.

194 Der Zweck der Verarbeitung personenbezogener Daten ist die Erfüllung eines Vertrags mit einem juristischen Partner des Unternehmens, Geschäftsbeziehungen.

195 Die Empfänger der personenbezogenen Daten sind die Mitarbeiter des Unternehmens, die kaufmännische und kundenbezogene Aufgaben wahrnehmen.

196 Dauer der Speicherung personenbezogener Daten: 5 Jahre nach Begründung der Geschäftsbeziehung oder der Eigenschaft der betroffenen Person als Vertreter.

TEIL VIII

VERARBEITUNG AUFGRUND DER ERFÜLLUNG EINER RECHTLICHEN VERPFLICHTUNG

30. zur Erfüllung von Steuer-, Beitrags- und Buchführungspflichten

197 Das Unternehmen verarbeitet die Daten natürlicher Personen, die mit dem Unternehmen als Kunden oder Lieferanten in geschäftlicher Beziehung stehen, zur Erfüllung seiner gesetzlichen, steuerlichen, beitragsrechtlichen und buchhalterischen Pflichten (Buchhaltung, Steuern), wie sie im Gesetz festgelegt sind.

§ des Gesetzes aus dem Jahr 2000 über die Buchhaltung: Name, Adresse, Bezeichnung der Person oder Organisation, die die Transaktion in Auftrag gegeben hat, Unterschrift der

Person, die die Transaktion in Auftrag gegeben hat, und der Person, die die Ausführung des Auftrags bescheinigt, sowie je nach Organisation die Unterschrift des Kontrolleurs; auf den Quittungen über Lagerbewegungen und Kassenbelegen die Unterschrift des Empfängers und auf den Gegenscheinen die Unterschrift des Zahlers und gemäß dem Gesetz CXVII aus dem Jahr 1995 über die Einkommensteuer (im Folgenden: Gesetz über die Einkommensteuer): die Nummer des Unternehmerausweises, die Nummer des Landwirteausweises, die Steueridentifikationsnummer.

(199) Die Aufbewahrungsfrist für personenbezogene Daten beträgt 8 Jahre nach Beendigung des Rechtsverhältnisses, auf das sich die Rechtsgrundlage stützt.

200 Die mit dieser Adresse verbundenen personenbezogenen Daten können von den Mitarbeitern des Unternehmens und den Datenverarbeitern verarbeitet werden, die Steuer-, Buchhaltungs-, Lohnbuchhaltungs- und Sozialversicherungsaufgaben wahrnehmen.

31 Verarbeitung der Daten des Arbeitsverhältnisses

201 Das Unternehmen verarbeitet die Daten von Arbeitnehmern zur rechtmäßigen Erfüllung einer gesetzlichen Verpflichtung und zur rechtmäßigen Erfüllung eines Arbeitsverhältnisses.

202. Abschnitt 134 (1) (c) und weitere Bestimmungen des Gesetzes. Die Dauer der Datenverarbeitung beträgt 8 Jahre.

203. § 134 (1) a) und weitere Bestimmungen des Gesetzes. Die Dauer der Datenverarbeitung beträgt 8 Jahre.

204. Artikel 56 und weitere Bestimmungen des Gesetzes. Die Dauer der Datenverarbeitung beträgt 50 Jahre.

Die Rechtsgrundlage für die Verarbeitung, der Zweck der Verarbeitung und der Umfang der im Zusammenhang mit dem Schaden des Opfers verarbeiteten Daten sind im Mt. Kapitel XIII und weiteren Bestimmungen des Gesetzes festgelegt. Die Dauer der Datenverarbeitung beträgt 50 Jahre. Wenn das Unternehmen einen Haftpflichtversicherungsvertrag abgeschlossen hat, sollte mit der Haftpflichtversicherungsgesellschaft ein gemeinsamer Vertrag mit dem für die Datenverarbeitung Verantwortlichen geschlossen werden.

(206) Im Falle eines Entschädigungsverfahrens für Schäden, die einem Arbeitgeber entstanden sind, sind die Rechtsgrundlage für die Verarbeitung, der Zweck der Verarbeitung und der Umfang der verarbeiteten Daten im Arbeitsgesetzbuch festgelegt. Kapitel XIV und weitere Bestimmungen des Gesetzes. Die Dauer der Datenverarbeitung beträgt 50 Jahre.

Hat das Unternehmen einen Schaden-/Unfallversicherungsvertrag abgeschlossen, sollte mit der Versicherungsgesellschaft ein Vertrag über die gemeinsame Datenverarbeitung geschlossen werden.

207 Die Rechtsgrundlage für die Datenverarbeitung im Zusammenhang mit Arbeitsunfällen, der Zweck der Datenverarbeitung und der Umfang der verarbeiteten Daten sind in Artikel 7, Artikel 49 und weiteren Bestimmungen des Gesetzes XCIII von 1993 über Sicherheit und Gesundheitsschutz am Arbeitsplatz festgelegt. Die Dauer der Datenverarbeitung beträgt 50 Jahre. Wenn das Unternehmen einen Haftpflichtversicherungsvertrag abgeschlossen hat, sollte mit der Haftpflichtversicherungsgesellschaft ein gemeinsamer Vertrag über die Datenverarbeitung geschlossen werden.

Die Rechtsgrundlage für die Verarbeitung der Daten von Personen, die Schulungen durchführen, der Zweck der Verarbeitung und der Umfang der verarbeiteten Daten werden durch das Gesetz CLXXXVII von 2011 und die weiteren Bestimmungen des Gesetzes bestimmt. Die Dauer der Datenverarbeitung beträgt 3 Jahre. Es sollte ein gemeinsamer Datenverwaltungsvertrag mit der an der Berufsausbildung beteiligten Bildungseinrichtung abgeschlossen werden.

209 Personenbezogene Daten zu dieser Adresse können von Mitarbeitern des Unternehmens, die Personalaufgaben wahrnehmen, oder von gemeinsam für die Verarbeitung Verantwortlichen verarbeitet werden.

32. die Verarbeitung von Zahlerdaten

210 Die Gesellschaft verarbeitet die personenbezogenen Daten der betroffenen Personen - Angestellte, deren Familienangehörige, Arbeitnehmer, sonstige Begünstigte -, mit denen sie als Zahlstelle in Beziehung steht (Art. 7, Punkt 31 des Gesetzes Nr. CL von 2017 über die Steuerordnung), zum Zwecke der Erfüllung der gesetzlich vorgesehenen Steuer- und Beitragspflichten (Steuern, Steuervorauszahlungen, Beiträge, Lohnbuchhaltung, Sozialversicherung, Rentenverwaltung). Der Umfang der verarbeiteten Daten ist in Art. 50 des Art. Wenn die Steuergesetze eine Rechtsfolge vorsehen, kann das Unternehmen Daten über die Gesundheitsfürsorge der Arbeitnehmer (§ 40 des Steuergesetzes) und die Mitgliedschaft in einer Gewerkschaft (§ 47 Absatz 2 Buchstabe b des Gewerkschaftsgesetzes) für die Zwecke der Erfüllung der Steuer- und Beitragspflichten (Lohn- und Gehaltsabrechnung, Verwaltung der Sozialversicherung) verarbeiten.

Die Rechtsgrundlage für die Verarbeitung von Daten im Zusammenhang mit dem Abzug von Sozialversicherungsbeiträgen, der Zweck der Verarbeitung und der Umfang der verarbeiteten Daten sind im Gesetz Nr. LXXX von 1997 über Sozialversicherungsrentenleistungen festgelegt.

212 Die Rechtsgrundlage für die Verarbeitung von Daten über Schulden von Arbeitnehmern, der Zweck der Verarbeitung und der Umfang der verarbeiteten Daten sind in den Artikeln 24 bis 28 des Gesetzes LIII von 1994 über die gerichtliche Vollstreckung und in weiteren Bestimmungen des Gesetzes festgelegt.

213 Die Rechtsgrundlage für die Verarbeitung von Daten zum Zweck der Entsendung, der Zweck der Verarbeitung und der Umfang der verarbeiteten Daten sind in Sjjatv. 3 §§ 10, 11, 12, 83 und weiteren Bestimmungen des Gesetzes festgelegt.

Die Rechtsgrundlage für die Verarbeitung von Daten im Zusammenhang mit Kantinenleistungen, der Zweck der Verarbeitung und der Umfang der verarbeiteten Daten sind in § 71 des Gesetzes über den Schutz personenbezogener Daten und anderen Bestimmungen des Gesetzes festgelegt. Das Unternehmen schließt eine gemeinsame Datenverarbeitungsvereinbarung mit den Anbietern des Kantinendienstes ab.

Die Rechtsgrundlage für die Verarbeitung von Daten im Zusammenhang mit Unfallleistungen, der Zweck der Verarbeitung und der Umfang der verarbeiteten Daten sind in Kapitel VI des Gesetzes Nr. LXXXIII von 1997 über Leistungen der obligatorischen Krankenversicherung (im Folgenden: "Gesetz über Leistungen der obligatorischen Krankenversicherung") und in den weiteren Bestimmungen des Gesetzes festgelegt.

216 Die Rechtsgrundlage für die Verarbeitung von Daten im Zusammenhang mit der Zahlung von Sozialversicherungsleistungen, der Zweck der Verarbeitung und der Umfang der verarbeiteten Daten sind in den Artikeln 40-42 des Beschäftigungsgesetzes und in weiteren Bestimmungen des Gesetzes festgelegt.

217. § 134 (1) c) und weitere Bestimmungen des Gesetzes.

Die Rechtsgrundlage für die Verarbeitung von Daten im Zusammenhang mit der Zahlung von Geldleistungen, der Zweck der Verarbeitung und der Umfang der verarbeiteten Daten sind in Artikel 43 des Gesetzes LXXXIII von 1997 und in den weiteren Bestimmungen des Gesetzes festgelegt.

219 Die Aufbewahrungsfrist für personenbezogene Daten beträgt 8 Jahre nach Beendigung des Rechtsverhältnisses, auf das sich die Rechtsgrundlage stützt.

220 Personenbezogene Daten können von Mitarbeitern des Unternehmens und von Datenverarbeitern verarbeitet werden, die Aufgaben in den Bereichen Steuern, Gehaltsabrechnung und Sozialversicherung (Lohnbuchhaltung) wahrnehmen.

33. die Bearbeitung von Dokumenten mit dauerhaftem Wert

221 Das Unternehmen verwaltet seine Dokumente von bleibendem Wert gemäß dem Gesetz LXVI von 1995 über öffentliche Aufzeichnungen, öffentliche Archive und den Schutz von privatem Archivgut, um zu gewährleisten, dass der Teil seines Archivmaterials von bleibendem Wert unversehrt und in einem für künftige Generationen nutzbaren Zustand erhalten bleibt. Dauer der Aufbewahrung: bis zur Übergabe an das öffentliche Archiv.

222 Die personenbezogenen Daten können vom Leiter des Unternehmens, von den Mitarbeitern des Unternehmens, die mit der Verwaltung und Archivierung der Dokumente betraut sind, sowie von den Mitarbeitern des öffentlichen Archivs verarbeitet werden.

34 Datenverarbeitung im Zusammenhang mit Verpflichtungen zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung und restriktiven Maßnahmen

223.) verarbeitet das Unternehmen die angegebenen Daten seiner Kunden, ihrer Vertreter und wirtschaftlichen Eigentümer (Name, Vorname, Name und Vorname bei der Geburt, Staatsangehörigkeit, Geburtsort und -datum, Name der Mutter bei der Geburt, Anschrift oder, in Ermangelung dessen, Wohnort, Art und Nummer des Ausweises; Nummer des amtlichen Personalausweises zum Nachweis der Anschrift).

Das Unternehmen verarbeitet die im Gesetz LII von 2017 über die Umsetzung der von der Europäischen Union und dem Sicherheitsrat der Vereinten Nationen verhängten restriktiven Finanz- und Eigentumsmaßnahmen (Kit) genannten Daten für die im Gesetz genannten Zwecke (Name, Vorname, Name und Vorname bei der Geburt, Staatsangehörigkeit, Geburtsort und -datum, Name der Mutter bei der Geburt, Adresse oder, in Ermangelung dessen, Wohnort, Art und Nummer des Ausweises). Gemäß Artikel 16 Absatz 5 des Gesetzes beträgt die Schutzdauer der Daten 10 Jahre.

225 Die personenbezogenen Daten können vom Geschäftsführer des Unternehmens, von seinen Mitarbeitern, die Aufgaben im Zusammenhang mit dem Kundendienst wahrnehmen, oder von einer vom Unternehmen benannten Person verarbeitet werden.

35. allgemeine Bedingungen für die Datenverarbeitung

226 Das Unternehmen schließt einen schriftlichen Vertrag über die Datenverarbeitungstätigkeit ab.

227 Die allgemeinen Bedingungen für die Datenverarbeitungstätigkeiten des Unternehmens sind in Anhang 16 aufgeführt.

228 Der Inhalt der allgemeinen Geschäftsbedingungen muss der anderen Partei vor Vertragsabschluss bekannt gegeben und von ihr akzeptiert werden.

TEIL X

UMGANG MIT DATENSCHUTZVERLETZUNGEN

36. der Begriff der Verletzung des Schutzes personenbezogener Daten

Der Begriff der Verletzung des Schutzes personenbezogener Daten ist in Artikel 4 Absatz 12 der Datenschutz-Grundverordnung festgelegt. Ein Datenschutzvorfall kann beispielsweise sein: Verlust eines USB-Sticks, eines Laptops oder eines Mobiltelefons; Verlust personenbezogener Daten; unsichere Speicherung personenbezogener Daten (z. B. in den Müll geworfene Zahlungsbelege); unsichere Übermittlung von Daten (fehlgeleitete E-Mails); unbefugtes Kopieren oder Übermitteln von Kunden- und Kundenpartnerlisten; Angriffe auf Server; Hacking einer Website; Nichtverfügbarkeit eines IT-Systems, das personenbezogene Daten verarbeitet; Offenlegung personenbezogener Daten.

37. die Behandlung und Behebung von Datenschutzvorfällen

230 Die Vorbeugung und Behandlung von Datenschutzvorfällen, die Einhaltung der einschlägigen Rechtsvorschriften und die Überwachung liegen in der Verantwortung der Unternehmensleitung.

231 Zugriffe und Zugriffsversuche auf IT-Systeme sollten protokolliert und laufend analysiert werden.

Wenn die mit der Aufsicht betrauten Mitarbeiter des Unternehmens von einem Datenschutzvorfall Kenntnis erhalten, sollten sie unverzüglich den Leiter des Unternehmens informieren.

233 Die Mitarbeiter des Unternehmens müssen dem Vorgesetzten oder der Person, die die Rechte des Arbeitgebers wahrnimmt, schriftlich Bericht erstatten, wenn sie von einem Datenschutzvorfall oder einem Ereignis, das auf einen solchen Vorfall hindeuten könnte, Kenntnis erhalten.

234 Die Datenschutzverletzung kann an die zentrale E-Mail-Adresse und Telefonnummer des Unternehmens gemeldet werden.

235 Im Falle einer Meldung einer Datenschutzverletzung wird der Leiter des Unternehmens unter Einbeziehung des Leiters der IT-Abteilung, des Finanzleiters und des Betriebsleiters die Meldung unverzüglich untersuchen.

236 Bei der Voruntersuchung ist zu entscheiden, ob es sich um einen echten Vorfall oder um eine Falschmeldung handelt. An der Voruntersuchung beteiligt der Verwalter den Verwalter, erforderlichenfalls den DSB oder den Datenverarbeiter und den Verantwortlichen für die Kontrolle der Verarbeitung personenbezogener Daten.

237. zu prüfen und zu bestimmen:

a) die Art des Vorfalls

b) die Zeit und den Ort des Ereignisses,

c) die Umstände und Auswirkungen des Vorfalls,

d) den Umfang und die Menge der während des Vorfalls kompromittierten Daten,

(e) die von den kompromittierten Daten betroffenen Personen,

(f) eine Beschreibung der Maßnahmen, die zur Behebung des Vorfalls getroffen wurden,

g) eine Beschreibung der Maßnahmen, die zur Vermeidung, Behebung oder Verringerung des Schadens ergriffen wurden.

238 Wenn der Datenschutzvorfall der Aufsichtsbehörde (NAIH) gemeldet werden muss, ergreift der Leiter des Unternehmens die erforderlichen Maßnahmen.

239 Im Falle einer Datenpanne müssen die betroffenen Systeme, Personen und Daten eingegrenzt und isoliert werden, und die Beweise, die die Panne belegen, müssen gesammelt und gesichert werden. Anschließend können die Schadensbehebung und die Rückkehr zum rechtmäßigen Betrieb beginnen.

240 Wenn der Verdacht besteht, dass es sich bei der Datenverletzung um eine Straftat handelt, wird das Unternehmen Strafanzeige erstatten.

38. die Aufzeichnungen über Datenschutzvorfälle

(241) Aufzeichnungen über Datenschutzvorfälle sind gemäß Anhang 2 zu führen und müssen Folgendes enthalten

a) die Art des Vorfalls,

b) die Kategorien und die Anzahl der betroffenen personenbezogenen Daten,

c) den Umfang und die Anzahl der von der Datenschutzverletzung betroffenen Personen,

d) das Datum und die Umstände, unter denen die Datenverletzung bekannt wurde,

e) die Umstände und Auswirkungen der Verletzung des Schutzes personenbezogener Daten,

f) die Maßnahmen, die zur Behebung der Datenschutzverletzung ergriffen wurden,

g) das Datum der Notifizierung,

(h) sonstige Daten, die in den Rechtsvorschriften, die die Verarbeitung vorschreiben, aufgeführt sind.

242 Die Daten über Datenschutzvorfälle im Register müssen 5 Jahre lang aufbewahrt werden.

TEIL XI

DATENSCHUTZ-FOLGENABSCHÄTZUNG

39. datenschutzrechtliche Folgenabschätzung und vorherige Konsultation

(243) Kann eine Verarbeitung, insbesondere eine Verarbeitung unter Einsatz neuer Technologien, unter Berücksichtigung ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen bergen, so führt der für die Verarbeitung Verantwortliche vor der Verarbeitung eine Folgenabschätzung durch, um zu bewerten, wie sich die geplanten Verarbeitungen auf den Schutz personenbezogener Daten auswirken werden. Ähnliche Arten von Verarbeitungen, die ähnlich hohe Risiken aufweisen, können im Rahmen einer einzigen Folgenabschätzung bewertet werden.

244 Der Leiter des Unternehmens ist für die Beauftragung der Datenschutz-Folgenabschätzung verantwortlich. Der Rat des behördlichen Datenschutzbeauftragten, sofern er bestellt ist, sollte eingeholt werden.

Kommt die Datenschutz-Folgenabschätzung zu dem Schluss, dass die Verarbeitung wahrscheinlich ein hohes Risiko zur Folge hat, wenn der für die Verarbeitung Verantwortliche keine Maßnahmen zur Risikominderung ergreift, konsultiert er die Aufsichtsbehörde, bevor er die personenbezogenen Daten verarbeitet.

246 Die Einzelheiten der Datenschutz-Folgenabschätzung und der vorherigen Konsultation sind in den Artikeln 35-36 der Verordnung und in den Bestimmungen des Infotv geregelt.

TEIL XII

DIE RECHTE DER BETROFFENEN PERSON

40. die Information über die Rechte der betroffenen Person

247 Ein Hinweis auf die Rechte der betroffenen Personen sollte auf der Website des Unternehmens veröffentlicht und gepflegt werden.

248 Anfragen zur Datenverarbeitung sind an den Leiter des Unternehmens zu richten, der dafür sorgt, dass sie innerhalb der Fristen beantwortet werden.

249 In jedem Fall ist zu prüfen, ob die Person, die die Rechte ausüben will, dazu berechtigt ist. Zu diesem Zweck müssen die personenbezogenen Daten der betroffenen Person im Zusammenhang mit der Ausübung des Rechts zuvor überprüft werden

250 Bei der Ausübung dieser Rechte dürfen die Rechte und Freiheiten anderer nicht verletzt werden, und das Unternehmen stellt sicher, dass alle Daten, die nicht offengelegt werden können, anonymisiert werden.

(251) Das Unternehmen bezieht den DSB in die Ausarbeitung des Entwurfs der Antwort an die betroffene Person ein, damit die betroffene Person ihre Rechte in angemessener Weise und im erforderlichen Umfang ausüben kann.

252 Die betroffene Person kann ihre Rechte unentgeltlich ausüben. Im Falle eines Missbrauchs, insbesondere bei wiederholten Anfragen nach denselben Daten, kann eine Gebühr erhoben werden.

253 Rechte der betroffenen Person:

a) transparente Information, Kommunikation und Erleichterung der Ausübung der Rechte der betroffenen Person;

b) Vorabinformation - wenn die personenbezogenen Daten bei der betroffenen Person erhoben werden;

(c) Unterrichtung der betroffenen Person, wenn die personenbezogenen Daten nicht bei ihr erhoben wurden;

d) das Recht auf Zugang;

e) das Recht auf Berichtigung;

f) das Recht auf Löschung (Recht auf Vergessenwerden);

(g) das Recht auf Einschränkung der Verarbeitung;

(h) das Recht, über die Berichtigung, Löschung oder Einschränkung der Verarbeitung informiert zu werden;

i) das Recht auf Datenübertragbarkeit;

j) das Recht, Einspruch zu erheben;

k) automatisierte Entscheidungsfindung in Einzelfällen, einschließlich Profiling;

l) Einschränkungen;

(m) Informationen über die Datenschutzverletzung;

(n) das Recht, eine Beschwerde bei der Aufsichtsbehörde einzureichen (Beschwerderecht bei der Behörde);

(o) das Recht auf einen gerichtlichen Rechtsbehelf gegen die Aufsichtsbehörde;

(p) das Recht auf Rechtsbehelf gegen den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter;

41. transparente Information, Kommunikation und Unterstützung bei der Ausübung der Rechte der Betroffenen

Der für die Verarbeitung Verantwortliche muss der betroffenen Person unentgeltlich alle Informationen und Angaben über die Verarbeitung personenbezogener Daten in knapper, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung stellen, insbesondere im Falle von Informationen, die sich an Kinder richten. Die Informationen werden schriftlich oder in anderer dokumentierter Form,

gegebenenfalls auch in elektronischer Form, erteilt. Auf Antrag der betroffenen Person kann die Auskunft mündlich erteilt werden, sofern die Identität der betroffenen Person auf andere Weise überprüft worden ist.

(255) Der für die Verarbeitung Verantwortliche erleichtert der betroffenen Person die Ausübung ihrer Rechte, indem er den DSB konsultiert, um dies sicherzustellen.

(256) Der für die Verarbeitung Verantwortliche unterrichtet die betroffene Person unverzüglich, spätestens jedoch innerhalb eines Monats nach Eingang des Antrags, über die Maßnahmen, die auf ihren Antrag auf Ausübung ihrer Rechte hin getroffen wurden. Diese Frist kann unter den in der Datenschutz-Grundverordnung festgelegten Bedingungen um weitere zwei Monate verlängert werden. Die betroffene Person wird innerhalb eines Monats über die Verlängerung und die Gründe dafür unterrichtet.

(257) Wird der für die Verarbeitung Verantwortliche dem Antrag der betroffenen Person nicht gerecht, so teilt er ihr unverzüglich, spätestens jedoch innerhalb eines Monats nach Eingang des Antrags, die Gründe für die Untätigkeit mit und weist sie auf die Möglichkeit hin, bei einer Aufsichtsbehörde Beschwerde einzulegen und ihr Recht auf einen gerichtlichen Rechtsbehelf wahrzunehmen.

Der für die Verarbeitung Verantwortliche erteilt die Auskünfte sowie die Informationen und Maßnahmen zu den Rechten der betroffenen Person unentgeltlich, kann jedoch eine Gebühr in Höhe der Verwaltungskosten erheben, wenn der Antrag offensichtlich unbegründet oder überzogen ist.

42. das Recht auf vorherige Information, wenn personenbezogene Daten bei der betroffenen Person erhoben werden

259 Die betroffene Person hat das Recht, vor der Verarbeitung der folgenden Daten über die Fakten und Informationen im Zusammenhang mit der Verarbeitung informiert zu werden:

a) die Identität und die Kontaktdaten des für die Verarbeitung Verantwortlichen und seines Vertreters,

b) die Kontaktdaten des Datenschutzbeauftragten (falls vorhanden),

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, und die Rechtsgrundlage für die Verarbeitung,

(d) im Falle einer Verarbeitung auf der Grundlage berechtigter Interessen: die berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten,

e) die Empfänger der personenbezogenen Daten, an die die personenbezogenen Daten weitergegeben werden, und gegebenenfalls die Kategorien von Empfängern;

e) die Tatsache, dass der für die Verarbeitung Verantwortliche beabsichtigt, die personenbezogenen Daten in ein Drittland oder an eine internationale Organisation zu übermitteln.

260 Um eine faire und transparente Verarbeitung zu gewährleisten, muss der für die Verarbeitung Verantwortliche der betroffenen Person die folgenden zusätzlichen Informationen zur Verfügung stellen:

(a) die Dauer der Speicherung der personenbezogenen Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

(b) das Recht der betroffenen Person, von dem für die Verarbeitung Verantwortlichen Zugang zu den sie betreffenden personenbezogenen Daten zu verlangen, sie zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken sowie Widerspruch gegen die Verarbeitung dieser personenbezogenen Daten einzulegen, sowie das Recht der betroffenen Person auf Datenübertragbarkeit;

(c) im Falle einer Verarbeitung, die auf der Einwilligung der betroffenen Person beruht, das Recht, die Einwilligung zu widerrufen, wobei die Rechtmäßigkeit der vor dem Widerruf erfolgten Verarbeitung unberührt bleibt;

(d) das Recht, eine Beschwerde bei einer Aufsichtsbehörde einzureichen;

(e) ob die Bereitstellung der personenbezogenen Daten auf einer gesetzlichen oder vertraglichen Verpflichtung beruht oder eine Voraussetzung für den Abschluss eines Vertrags ist, ob die betroffene Person zur Bereitstellung der personenbezogenen Daten verpflichtet ist und welche Folgen die Nichtbereitstellung der Daten haben kann;

(f) die Tatsache, dass eine automatisierte Entscheidungsfindung, einschließlich Profiling, stattfindet, und zumindest in diesen Fällen die verwendete Logik sowie klare Informationen über die Bedeutung einer solchen Verarbeitung und die voraussichtlichen Folgen für die betroffene Person.

Beabsichtigt der für die Verarbeitung Verantwortliche, personenbezogene Daten für einen anderen Zweck als den, für den sie erhoben wurden, weiterzuverarbeiten, so muss er die betroffene Person vor der Weiterverarbeitung über den anderen Zweck und alle relevanten zusätzlichen Informationen, die im vorstehenden Punkt beschrieben sind, informieren.

43. die Unterrichtung der betroffenen Person, wenn die personenbezogenen Daten nicht bei ihr erhoben worden sind

262. Hat der für die Verarbeitung Verantwortliche die personenbezogenen Daten nicht bei der betroffenen Person erhoben, so teilt er ihr dies spätestens einen Monat nach Erhebung der personenbezogenen Daten mit; werden die personenbezogenen Daten zum Zwecke der Kontaktaufnahme mit der betroffenen Person verwendet, so spätestens bei der ersten Kontaktaufnahme mit der betroffenen Person; oder, falls die Daten an einen anderen Empfänger weitergegeben werden sollen, spätestens zum Zeitpunkt der ersten Weitergabe der personenbezogenen Daten, die in den ersten beiden Punkten der vorstehenden Überschrift beschriebenen Fakten und Informationen, die Kategorien der betroffenen

personenbezogenen Daten und die Quelle der personenbezogenen Daten sowie gegebenenfalls die Angabe, ob die Daten aus öffentlich zugänglichen Quellen stammen.

(263) Die übrigen Regeln sind die in den ersten beiden Punkten des vorstehenden Titels genannten.

44 Recht auf Auskunft der betroffenen Person

Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen eine Rückmeldung darüber zu erhalten, ob ihre personenbezogenen Daten verarbeitet werden, und, falls dies der Fall ist, das Recht auf Auskunft über die personenbezogenen Daten und die damit zusammenhängenden Informationen, wie in Punkt 1 des Rechts auf vorherige Information beschrieben.

(265) Werden personenbezogene Daten an ein Drittland oder eine internationale Organisation übermittelt, hat die betroffene Person das Recht, über die für die Übermittlung geltenden Garantien gemäß Artikel 46 DSGVO informiert zu werden.

(266) Der für die Verarbeitung Verantwortliche stellt der betroffenen Person eine Kopie der verarbeiteten personenbezogenen Daten zur Verfügung. Für zusätzliche Kopien, die von der betroffenen Person angefordert werden, kann der für die Verarbeitung Verantwortliche eine angemessene Gebühr auf der Grundlage der Verwaltungskosten erheben.

45. das Recht auf Berichtigung

(267) Die betroffene Person hat das Recht, auf Antrag und ohne unangemessene Verzögerung von dem für die Verarbeitung Verantwortlichen die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.

268 Vorbehaltlich der Zwecke der Verarbeitung hat die betroffene Person auch das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen, auch mittels einer ergänzenden Erklärung.

46 Recht auf Löschung ("Recht auf Vergessenwerden")

(269) Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der für die Verarbeitung Verantwortliche ist verpflichtet, sie betreffende personenbezogene Daten unverzüglich zu löschen, wenn.

(a) die personenbezogenen Daten für die Zwecke, für die sie erhoben oder anderweitig verarbeitet wurden, nicht mehr erforderlich sind;

(b) die betroffene Person ihre Einwilligung zu der Verarbeitung widerruft und es keine andere Rechtsgrundlage für die Verarbeitung gibt;

(c) die betroffene Person Widerspruch gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe für die Verarbeitung vorliegen,

d) die personenbezogenen Daten unrechtmäßig verarbeitet worden sind;

(e) die personenbezogenen Daten müssen gelöscht werden, um einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten nachzukommen, dem der für die Verarbeitung Verantwortliche unterliegt;

f) die personenbezogenen Daten wurden im Zusammenhang mit der Bereitstellung von Diensten der Informationsgesellschaft direkt für ein Kind erhoben.

270 Das Recht auf Löschung kann nicht ausgeübt werden, wenn die Verarbeitung erforderlich ist

a) für die Ausübung des Rechts auf Meinungs- und Informationsfreiheit;

(b) zur Erfüllung einer rechtlichen Verpflichtung, der der für die Verarbeitung Verantwortliche unterliegt, oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;

c) auf der Grundlage des öffentlichen Interesses im Bereich der öffentlichen Gesundheit;

(d) zu im öffentlichen Interesse liegenden Zwecken der Archivierung, der wissenschaftlichen oder historischen Forschung oder der Statistik, wenn das Recht auf Löschung eine solche Verarbeitung unmöglich machen oder ernsthaft gefährden würde, oder

(e) für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

47. das Recht auf Einschränkung der Verarbeitung

(271) Die betroffene Person hat das Recht, auf Antrag von dem für die Verarbeitung Verantwortlichen eine Einschränkung der Verarbeitung zu verlangen, wenn:

(a) die betroffene Person bestreitet die Richtigkeit der personenbezogenen Daten; in diesem Fall bezieht sich die Einschränkung auf den Zeitraum, in dem der für die Verarbeitung Verantwortliche die Richtigkeit der personenbezogenen Daten überprüfen kann;

(b) die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der Daten ablehnt und stattdessen die Einschränkung ihrer Verwendung verlangt;

(c) der für die Verarbeitung Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht mehr benötigt, die betroffene Person sie aber zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt; oder

(d) die betroffene Person hat gegen die Verarbeitung Widerspruch eingelegt; in diesem Fall gilt die Einschränkung für den Zeitraum, bis festgestellt ist, ob die berechtigten Gründe des für die Verarbeitung Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

(272) Im Falle einer Einschränkung der Verarbeitung dürfen personenbezogene Daten, abgesehen von ihrer Speicherung, nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte von Personen oder wichtiger öffentlicher Interessen verarbeitet werden.

273 Die betroffene Person muss im Voraus über die Aufhebung der Einschränkung der Verarbeitung informiert werden.

48 Pflicht zur Meldung der Berichtigung, Löschung oder Einschränkung der Verarbeitung

Der für die Verarbeitung Verantwortliche unterrichtet jeden Empfänger über die Berichtigung, Löschung oder Einschränkung der Verarbeitung, an den oder dem die personenbezogenen Daten übermittelt wurden, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der für die Verarbeitung Verantwortliche unterrichtet die betroffene Person auf deren Antrag über diese Empfänger.

49. das Recht auf Datenübertragbarkeit

275 Das Unternehmen verarbeitet keine Daten, die auf automatisierten Entscheidungen beruhen, so dass das Recht auf Datenübertragbarkeit nicht ausgeübt werden kann.

50. das Recht auf Widerspruch

276 Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund berechtigter Interessen erfolgt, Widerspruch einzulegen; dies gilt auch für ein Profiling. In diesem Fall darf der für die Verarbeitung Verantwortliche die personenbezogenen Daten nicht mehr verarbeiten, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

(277) Werden personenbezogene Daten für Zwecke der Direktwerbung verarbeitet, so hat die betroffene Person das Recht, Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht. Widerspricht die betroffene Person der Verarbeitung

personenbezogener Daten für Zwecke der Direktwerbung, so dürfen die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet werden.

278 Das in den beiden vorangegangenen Punkten dargelegte Recht muss der betroffenen Person spätestens beim ersten Kontakt mit ihr ausdrücklich zur Kenntnis gebracht werden, und die Informationen müssen deutlich getrennt von allen anderen Informationen angezeigt werden.

279 In Bezug auf die Dienste der Informationsgesellschaft kann die betroffene Person von ihrem Recht Gebrauch machen, auf der Grundlage technischer Spezifikationen Widerspruch gegen automatisierte Verfahren einzulegen.

(280) Werden personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitet, so hat die betroffene Person das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen, es sei denn, die Verarbeitung ist zur Erfüllung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt.

51. automatisierte Entscheidungsfindung, Profiling

281 Das Unternehmen verwendet keine automatisierte Datenverarbeitung.

52. einschränkungen

282. Das für den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter geltende Unionsrecht oder das Recht der Mitgliedstaaten kann in den in Artikel 23 der Datenschutz-Grundverordnung genannten Fällen den Umfang und die Tragweite der Rechte und Pflichten (Artikel 12 bis 22, 34, 5 der Verordnung) durch Rechtsetzungsmaßnahmen einschränken, sofern die Einschränkung den wesentlichen Inhalt der Grundrechte und -freiheiten wahrt.

53 Informationen über die Datenschutzverletzung

(283) Führt die Verletzung des Schutzes personenbezogener Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen, unterrichtet der für die Verarbeitung Verantwortliche die betroffene Person unverzüglich über die Verletzung des Schutzes personenbezogener Daten.

Die Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten muss klar und deutlich die Art der Verletzung des Schutzes personenbezogener Daten beschreiben und mindestens Folgendes enthalten:

(a) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer anderen Kontaktperson, die weitere Auskünfte erteilen kann;

c) die voraussichtlichen Folgen der Datenschutzverletzung;

(d) die Maßnahmen, die zur Behebung der Verletzung des Schutzes personenbezogener Daten ergriffen wurden oder geplant sind, gegebenenfalls einschließlich Maßnahmen zur Abmilderung etwaiger nachteiliger Folgen der Verletzung des Schutzes personenbezogener Daten.

(285) Die betroffene Person muss nicht informiert werden, wenn:

(a) der für die Verarbeitung Verantwortliche geeignete technische und organisatorische Schutzmaßnahmen getroffen hat und diese Maßnahmen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden, insbesondere Maßnahmen wie die Verwendung von Verschlüsselung, die die Daten für Personen, die nicht zum Zugriff auf die personenbezogenen Daten berechtigt sind, unverständlich machen;

(b) der für die Verarbeitung Verantwortliche nach der Verletzung des Schutzes personenbezogener Daten zusätzliche Maßnahmen ergriffen hat, um sicherzustellen, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person wahrscheinlich nicht mehr besteht;

c) die Unterrichtung würde einen unverhältnismäßigen Aufwand erfordern. In diesen Fällen wird die betroffene Person durch öffentlich zugängliche Informationen oder durch eine ähnliche Maßnahme, die eine ebenso wirksame Unterrichtung der betroffenen Person gewährleistet, unterrichtet.

54. das Recht auf Beschwerde bei der Aufsichtsbehörde (NAIH)

286 Die betroffene Person hat das Recht, sich bei der Aufsichtsbehörde (Nationale Behörde für Datenschutz und Informationsfreiheit) zu beschweren, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO verstößt. Die Aufsichtsbehörde, bei der die Beschwerde eingereicht wurde, ist verpflichtet, die betroffene Person über die verfahrensrechtlichen Entwicklungen in Bezug auf die Beschwerde und deren Ergebnis, einschließlich des Rechts auf einen gerichtlichen Rechtsbehelf, zu informieren.

55 Recht auf Rechtsbehelf gegen die Aufsichtsbehörde

(287) Unbeschadet anderer Rechtsbehelfe hat jede natürliche oder juristische Person das Recht, einen wirksamen gerichtlichen Rechtsbehelf gegen eine sie betreffende rechtsverbindliche Entscheidung der Aufsichtsbehörde einzulegen.

(288) Die betroffene Person hat das Recht, einen gerichtlichen Rechtsbehelf einzulegen, wenn die Aufsichtsbehörde die Beschwerde nicht bearbeitet oder die betroffene Person nicht innerhalb von drei Monaten über die verfahrensmäßigen Entwicklungen im Zusammenhang mit der eingelegten Beschwerde oder über das Ergebnis der Beschwerde unterrichtet.

289 Für Klagen gegen eine Aufsichtsbehörde sind die Gerichte des Mitgliedstaats zuständig, in dem die Aufsichtsbehörde ihren Sitz hat.

Wird ein Verfahren gegen eine Entscheidung einer Aufsichtsbehörde eingeleitet, zu der der Europäische Datenschutzausschuss zuvor eine Stellungnahme oder Entscheidung im Rahmen des Kohärenzverfahrens abgegeben hat, ist die Aufsichtsbehörde verpflichtet, diese Stellungnahme oder Entscheidung an das Gericht weiterzuleiten.

56 Recht auf Rechtsbehelf gegen den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter

291 Unbeschadet der verfügbaren außergerichtlichen Rechtsbehelfe, einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde, steht allen betroffenen Personen ein wirksamer gerichtlicher Rechtsbehelf zur Verfügung, wenn sie der Ansicht sind, dass ihre Rechte infolge der Verarbeitung ihrer personenbezogenen Daten unter Verstoß gegen die DSGVO verletzt wurden.

Klagen gegen den für die Verarbeitung Verantwortlichen oder den Auftragsverarbeiter sind bei den Gerichten des Mitgliedstaats zu erheben, in dem der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter niedergelassen ist. Diese Verfahren können auch bei den Gerichten des Mitgliedstaats anhängig gemacht werden, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat, es sei denn, bei dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter handelt es sich um eine Behörde eines Mitgliedstaats, die in Ausübung öffentlicher Gewalt handelt.

TEIL XIII

SCHLUSSBESTIMMUNGEN

57. die Aufstellung, Änderung und Einarbeitung der Geschäftsordnung

293 Der Leiter des Unternehmens ist befugt, die Geschäftsordnung zu erlassen und zu ändern.

294 Der Leiter des Unternehmens stellt sicher, dass die in der Datenschutzpolitik festgelegten Anforderungen in den Prozessen und der täglichen Arbeit des Unternehmens umgesetzt werden.

295 Diese Politik muss allen Mitarbeitern sowohl in elektronischer als auch in Papierform zur Verfügung gestellt werden.

296 Die Bestimmungen des Kodex sollten allen Mitarbeitern des Unternehmens mitgeteilt werden, und in den Arbeitsverträgen sollte festgelegt werden, dass die Einhaltung und Durchsetzung des Kodex ein wesentlicher Bestandteil der Arbeitspflichten aller Mitarbeiter ist. Ein Muster für einen Arbeitsvertragszusatz ist in Anhang 17 zu diesen Vorschriften enthalten.

297 Das Unternehmen ergänzt die Arbeitsverträge seiner Mitarbeiter auf der Grundlage dieser Politik und sorgt für Vertraulichkeit im Falle der Offenlegung personenbezogener Daten, die nicht mit dem Arbeitsverhältnis zusammenhängen.

298 In einer Änderung des Arbeitsvertrags kann eine Sanktion in Höhe von bis zu einem Monatsgrundgehalt für die Nichteinhaltung der Bestimmungen des Kodex vorgesehen werden, sofern der vom Arbeitnehmer verursachte Datenschutzvorfall mindestens der Datenschutzaufsichtsbehörde gemeldet werden muss.

299 Das Unternehmen wird im Falle eines Verstoßes gegen die Datenschutzvorschriften Strafanzeige gegen die betroffene Person erstatten.

Der Datenschutzbeauftragte oder eine andere bevollmächtigte Person schult neu eingestellte Personen, die im Rahmen ihrer Tätigkeit personenbezogene Daten verarbeiten, innerhalb von drei Arbeitstagen nach der Einstellung im Datenschutz und informiert sie über die erforderlichen Rechtsvorschriften, internen Standards und sonstigen Begleitmaterialien; die Prüfung erfolgt innerhalb einer Woche nach der Schulung.

301 Die Mitarbeiter des Unternehmens, die personenbezogene Daten verarbeiten, nehmen jährlich an einer Datenschutzschulung teil, die von einem Datenschutzbeauftragten durchgeführt wird. Die jährliche Schulung kann eine Übung zum Umgang mit Zwischenfällen (mit nicht realen Daten) beinhalten.

(302) Der betreffende Vorgesetzte sorgt für die Einhaltung der für ihn geltenden Datenschutzvorschriften und die Durchsetzung dieser Vorschriften in Bezug auf sein Personal. Die betreffende Führungskraft überwacht den ihren Zuständigkeitsbereich betreffenden Teil des Anhangs 1 und meldet der für das Register zuständigen Person alle Änderungen.

(303) Der Leiter des für die Verarbeitung Verantwortlichen kann ein gezieltes Audit der Datenschutzaktivitäten des für die Verarbeitung Verantwortlichen anordnen. Die Einhaltung der IT-Sicherheitsbedingungen ist halbjährlich zu überprüfen und die Ergebnisse sind dem Verantwortlichen mitzuteilen.