Datenschutzgrundverordnung – Code of Conduct für Internet Service Provider

Version 1.1. v. 16.06.2020

ISPA – Internet Service Providers Austria

Währinger Straße 3/18
1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

Präambel

Seit dem 25. Mai 2018 gilt die Datenschutzgrundverordnung (DSGVO) in Österreich und ist direkt anwendbar. Ziel der Verordnung ist der Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten und die Vereinheitlichung der Datenschutzstandards in Europa.

Die unterzeichnenden Unternehmen sind sich in diesem Zusammenhang ihrer Rolle hinsichtlich der Gewährleistung des Grundrechts auf Datenschutz bewusst und bekennen sich ausdrücklich zu ihrer gesellschaftlichen Verantwortung im Rahmen ihrer unternehmerischen Tätigkeit.

Durch Erarbeitung eines gemeinsamen Grundverständnisses der branchenspezifischen Ausgestaltung der in der DSGVO enthaltenen Erfordernisse bzw. Verpflichtungen für ISPs sowie durch die Vornahme notwendiger Präzisierungen, einhergehend mit der Übermittlung dieses Verständnisses an die Kundinnen und Kunden soll eine bestmögliche Umsetzung der DSGVO sowie Rechtssicherheit für ISPs gewährleistet werden. Diese Verhaltensregeln präzisieren die Anwendung der DSGVO. Da die Bestimmungen des TKG für ISP in vielen datenschutzrechtlichen Fragestellungen berücksichtigt werden müssen, wird hier hinsichtlich der branchenspezifischen Spezifikationen auch auf diese eingegangen.

Aus diesem Grund hat der Verband Internet Service Providers Austria (ISPA) als Vertretung der österreichischen Internetwirtschaft in Zusammenarbeit mit seinen Mitgliedern sowie weiteren maßgeblichen Interessensträgern die nachfolgenden Verhaltensregeln gemäß Artikel 40 DSGVO ausgearbeitet, welche bei Bedarf und nach erneuter Vorlage an die Datenschutzbehörde weiterentwickelt und ergänzt werden können.

Geltungsbereich

Diesen Verhaltensregeln können sich Internet Service Provider, welche öffentliche Kommunikationsnetze oder -dienste bereitstellen und über eine Allgemeingenehmigung im Sinne von § 15 TKG verfügen, unterwerfen (siehe dazu Punkt VII unten).

I. Infrastrukturbezogene Leistungsbeziehungen

1. Bei der Erbringung von Kommunikationsdiensten an Endkunden ist jener Betreiber, der die vertragliche Endkundenbeziehung hält, regelmäßig datenschutzrechtlicher Verantwortlicher, der Endnutzer Betroffener. Um Endkunden die Nutzung von Kommunikationsdiensten auch über die Grenzen der Infrastruktur ihres Vertragspartners hinweg zu ermöglichen ist es dabei notwendig, dass Betreiber durch vertragliche und technische Vorkehrungen sicherstellen, dass Endkunden-Services nahtlos über Netzgrenzen hinweg erbracht werden können.

2. Damit dies gewährleistet wird, unterliegt die Zusammenarbeit der Betreiber einem eigenen sektorspezifischen Regelwerk, das auf europäischer Ebene durch diverse Richtlinien und Verordnungen einen Rahmen vorgibt und in nationale Gesetze (wie das Telekommunikationsgesetz 2003 in Österreich) umgesetzt ist. Neben Verpflichtungen, die alle Betreiber treffen (wie die Verpflichtung zur Zusammenschaltung), gibt es spezielle Zugangsverpflichtungen für marktbeherrschende Betreiber.

3. Die Betreiber unterliegen zudem gemäß dem sektorspezifischen europäischen Rechtsrahmen auch einem engen Rechtsregime hinsichtlich der Ausgestaltung ihrer Geschäftsmodelle. Hierzu zählt insbesondere die Regulierung von Wettbewerb, Frequenzen, Universaldienst und Konsumentenschutz sowie spezielle sektorspezifische Datenschutzbestimmungen.

4. Auf Basis des sektorspezifischen Regelwerks haben sich freiwillige und verpflichtende Zugangs- und Verbindungsleistungen („ISP-Leistungen“) entwickelt, die am (Vorleistungs-)Markt angeboten und nachgefragt werden. Diese sorgen letztlich für das Funktionieren des gesamten Marktes, den Austausch von Informationen über die Netzkante des einzelnen Betreibers und dafür, dass Betreiber, die nicht selbst über die notwendige Infrastruktur verfügen, Zugang zu fremder Infrastruktur bekommen und so wiederum in die Lage versetzt werden, ihre Produkte und Services an ihre Endnutzer anzubieten.

5. Bei der Erbringung der ISP-Leistungen zwischen Betreibern werden personenbezogene Daten von Endnutzern verarbeitet. Die Verarbeitung dieser Daten ist erforderlich um das klassische Geschäftsmodell eines Betreibers zu ermöglichen, das wie folgt ausgestaltet ist:

6. Vertragspartner bei der Erbringung von ISP-Leistungen sind immer zwei Betreiber, die wiederum nicht unbedingt, aber potentiell über eigene Endnutzerbeziehungen verfügen. Es bestehen in dieser speziellen Leistungsbeziehung keine vertraglichen Beziehungen zwischen dem Endnutzer eines Betreibers und dem anderen beteiligten Betreiber. Jeder Betreiber, der eine ISP-Leistung erbringt („Betreiber“) verarbeitet hierfür personenbezogene Daten des Endkunden des Nachfragers der ISP-Leistungen („Nachfrager“) in seinem Netz entsprechend der eigenen gesetzlichen Verpflichtungen, Datenschutzmanagementsystemen und Datensicherheitsanforderungen. Diese Daten müssen verarbeitet werden, um die ISP-Leistung erbringen zu können.

7. In jenen Fällen, in welchen die ISP-Leistungen ausschließlich auf dem sektorspezifischen Regelwerk beruhen, werden die Mittel und Zwecke der Datenverarbeitung durch die entsprechenden Regulierungsvorgaben festgelegt. Die Rolle des datenschutzrechtlichen Verantwortlichen iSd Art 4 Z 7 DSGVO bestimmt sich damit jeweils nach den Kriterien der nationalen Regulierungsvorgaben. Entsprechende regulatorische Verpflichtungen bestehen insbesondere in §§ 92 TKG ff sowie in den jeweiligen Regulierungsbescheiden der Telekom Control Kommission (TKK), die die Verarbeitung von personenbezogenen Daten von Endnutzern im Rahmen von ISP-Leistungen regeln und sogar konkret anordnen.

8. Im Verhältnis der Betreiber untereinander bestehen dabei keine gegenseitigen Weisungsrechte hinsichtlich der Datenverarbeitung. Gleichzeitig verfügt der Nachfrager grundsätzlich über keine Auswahlmöglichkeiten hinsichtlich des Betreibers, sondern ist an jenen Betreiber der die zur Erbringung des Endkunden-Services notwendigen ISP-Leistungen anbietet bzw. über die notwendige Infrastruktur verfügt gebunden. Daher wird zwischen Nachfrager und Betreiber auch keine Auftragsdatenverarbeitungsbeziehung im Sinne des Art 28 DSGVO begründet. Eine über den Zweck der ISP-Leistung hinausgehende Verarbeitung der Daten durch den Erbringer der ISP-Leistung im eigenen Interesse erfolgt nicht. Vielmehr werden Mittel und Zwecke der Datenverarbeitung ausschließlich durch die nationalen und europäischen Regulierungsvorgaben definiert.

   Datenschutzrechtlicher Verantwortlicher für die Datenverarbeitung im Rahmen der Erbringung des Endkunden-Services bleibt somit jener Betreiber, welcher die vertragliche

Endkundenbeziehung hält. Der Erbringer der ISP-Leistung wiederum ist eigenverantwortlich für die Einhaltung der gesetzlichen Datenschutz- und Datensicherheitsvorschriften und unterliegt hier ausdrücklich keinen Weisungsrechten (etwa betreffend Datensicherheitsmaßnahmen).

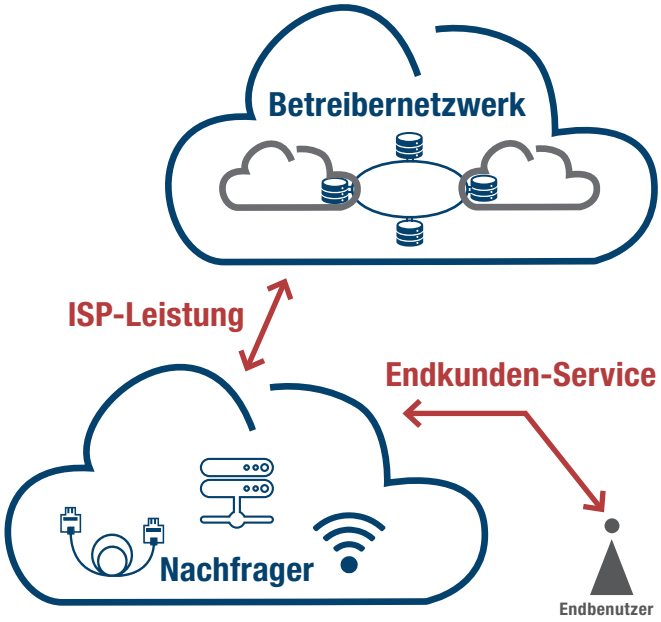
Festzuhalten ist auch, dass zwischen den Betreibern keine gemeinsame Verantwortlichkeit gemäß Art 26 DSGVO vorliegt, da hier Zwecke und Mittel zur Verarbeitung nicht gemeinsam festgelegt werden. Wie oben beschrieben, werden personenbezogene Daten von jedem Betreiber als Verantwortlicher für seine eigenen festgelegten Zwecke mit den von jedem Betreiber festgelegten bzw. durch allgemeine Standards vorgegebenen Mitteln verarbeitet.

9. Im Verhältnis gegenüber dem Endkunden ist der Betreiber, der die vertragliche Endkundenbeziehung hält, regelmäßig datenschutzrechtlicher Verantwortlicher, der Endnutzer Betroffener. Dies betrifft auch das Verhältnis gegenüber Geschäftskunden, welche selbst als datenschutzrechtlicher Verantwortlicher bezüglich eigener Datenanwendungen auftreten. Bei der Erbringung gewöhnlicher Kommunikationsdienste (Internetzugang, Telefonie...) unterliegt der Betreiber keinem Weisungsrecht des Endkunden, sondern verarbeitet personenbezogene Daten ausschließlich auf Grundlage der gesetzlichen und regulatorischen Vorgaben um die Leistung erbringen zu können. Es wird somit keine Auftragsdatenverarbeitungsbeziehung im Sinne des Art 28 DSGVO begründet.

   Auch in diesem Fall besteht keine gemeinsame Verantwortlichkeit gemäß Art 26 DSGV zwischen dem Betreiber und dem Endkunden. Allein der Betreiber legt sämtliche Zwecke und Mittel der Datenverarbeitung fest.

   Im Ausnahmefall kann jedoch das Angebot von Spezial- oder Zusatzservices eine Auftragsdatenverarbeitung begründen. Dies ist jedoch im Einzelfall zu beurteilen wobei speziell auf ein etwaiges vertragliches Weisungsverhältnis hinsichtlich der Datenverarbeitung abzustellen ist.

10. Neben jenen Leistungsbeziehungen, bei welchen Mittel und Zwecke der Datenverarbeitung ausschließlich durch die nationalen und europäischen Regulierungsvorgaben festgelegt sind, bestehen zudem noch weitere Zugangs- bzw. Verbindungsleistungen, welche nach dem gleichen Prinzip wie unter Pkt. 6 angeführt ablaufen. Hierbei handelt es sich um essentielle Leistungen, ohne die die Bereitstellung der Dienstleistung des Betreibers an den Endkunden nicht möglich wäre. Insbesondere besteht auch in diesen Fällen kein Weisungsrecht gegenüber dem Vertragspartner bzw. besteht nur eine stark eingeschränkte Auswahlmöglichkeit hinsichtlich des Vertragspartners. Eine über den Zweck der Erbringung der ISP-Leistung hinausgehende Verarbeitung der Daten durch den Erbringer der ISP-Leistung im eigenen Interesse erfolgt nicht. Auch in diesen Fällen ist jener Betreiber, welcher die Endkundenbeziehung hält, der datenschutzrechtliche Verantwortliche gegenüber dem Endkunden. Der Erbringer der ISP-Leistung wiederum ist eigenverantwortlich für die Einhaltung der gesetzlichen Datenschutz- und Datensicherheitsvorschriften zuständig.



(Abb. 1 Darstellung des ISP-Geschäftsmodells)

11. Verantwortlich für die Gewährung der Betroffenenrechte ist alleine der Nachfrager im Rahmen seines Endnutzervertragsverhältnisses. Die unterzeichnenden Betreiber stellen damit sicher, dass die Betroffenen bei ihrem direkten Vertragspartner eine dezidierte Ansprechstelle zur Wahrung und Durchsetzung ihrer Datenschutzrechte haben. Zudem ist auch nur der Nachfrager als direkter Vertragspartner des Betroffenen dazu im Stande, eine ausreichende Identifizierung des Betroffenen im Sinne des Art 11 Abs. 2 DSGVO durchzuführen, mit der sichergestellt wird, dass der Endnutzer seine Betroffenenrechte ausschließlich in Bezug auf die ihn betreffenden personenbezogenen Daten ausübt.

Beispielhafte Auflistung und Beschreibung von ISP-Leistungen

- **Zusammenschaltung** ist gemäß § 3 Z 25 TKG die physische und logische Verbindung öffentlicher Kommunikationsnetze, die von demselben oder einem anderen Unternehmen genutzt werden, um Nutzern eines Unternehmens die Kommunikation mit Nutzern desselben oder eines anderen Unternehmens oder den Zugang zu den von einem anderen Unternehmen angebotenen Diensten zu ermöglichen. Dienste können von den beteiligten Betreibern erbracht werden oder von anderen Betreibern, die Zugang zum Netz haben. Zusammenschaltung ist ein Sonderfall des Zugangs und wird zwischen Betreibern öffentlicher Netze hergestellt.
  Gemäß § 48 TKG 2003 ist jeder Betreiber eines öffentlichen Kommunikationsnetzes verpflichtet, anderen Betreibern solcher Netze auf Nachfrage ein Angebot auf Zusammenschaltung zu legen. Der Umfang der Zusammenschaltung ist in § 49 TKG 2003 geregelt. In diesem Umfang werden neben den Stammdaten des Vertragspartners die notwendigen Verkehrsdaten (Vermittlungsdaten der jeweiligen Verbindung oder Routingdaten im Fall paketorientierter Dienste an den zusammenschaltenden Betreiber; Zustell-/Verbindungsdaten; Verrechnungsdaten) verarbeitet.
  Um die Übertragung von Rufnummern (Portierung) zu ermöglichen werden entsprechend den Bestimmungen der Kommunikationsparameter-, Entgelt- und Mehrwertdiensteverordnung 2009 (KEM-V) und der Nummernübertragungsverordnung 2012 (NÜV) Stamm- und Verrechnungsdaten verarbeitet.

- **IP-Peering** ist eine Verbindungsleistung auf Basis einer Vereinbarung („peering agreement“) bei welcher zwei ISPs ihre Kommunikationsnetze zum Datenaustausch miteinander verbinden, sich jedoch keine Kosten verrechnen. Hierdurch soll den Endnutzern eines ISPs der Zugang zu den jeweiligen Dienstleistungen des anderen ISPs ermöglicht werden. Gleichsam wie bei der Zusammenschaltung werden hierzu neben den Stammdaten des Vertragspartners die notwendigen Verkehrsdaten (Routingdaten) an den angeschlossenen Betreiber übermittelt.

- **IP-Transit** bezeichnet eine Dienstleistung, bei der Datenverkehr gegen Entgelt durch das eigene Netzwerk durchgeleitet wird. Bei den Vertragspartnern handelt es sich dabei meist um unterschiedlich große Betreiber, wobei der größere Betreiber dem kleineren Betreiber gegen Entgelt einen sogenannten „Uplink“ zur Verfügung stellt. Die Abrechnung erfolgt anhand der darüber geleiteten Datenmenge. Hierzu werden zum einen die Stammdaten der Vertragspartner sowie die Routingdaten bzw. Verrechnungsdaten verarbeitet.

- **National Roaming** bedeutet, dass das Mobiltelefon des Endkunden im Inland ein anderes Netz benutzt als das Netz jenes Betreibers, mit dem der Betroffene einen Mobilvertrag abgeschlossen hat.
  Um den Dienst erbringen zu können werden keine Daten verarbeitet, die eine direkte Identifizierung des Betroffenen ermöglichen, sondern nur die MSISDN (Mobile Subscriber Integrated Services Digital Network Number).

- **Mietleitungen** sind gemäß § 3 Z 12 TKG 2003 Einrichtungen, die transparente Übertragungskapazität zwischen Netzabschlusspunkten zur Verfügung stellen, jedoch ohne Vermittlungsfunktionen, die der Benutzer selbst als Bestandteil des Mietleitungsangebots steuern kann (on-demand switching).

  Mietleitungen umfassen insbesondere
  - die Zurverfügungstellung von Leitungen mit traditionellen Schnittstellen (Dienste ohne Vermittlungsfunktion, die transparente Übertragungskapazität zwischen Netzabschlusspunkten (symmetrisch bidirektional) zur Verfügung stellen)
  - Ethernetdienste (Dienste, die eine garantierte Bandbreite zwischen zwei Netzabschlusspunkten zur Verfügung stellen)
  - Unbeschaltete Glasfaser (= ein Glasfaserpaar, das unbeschaltet vermietet wird)

  Zusammengefasst sind Mietleitungen eine physikalische Verbindung zwischen zwei Punkten. Für die Erbringung der Services ist daher die Verarbeitung von standortbezogenen Informationen (Standortdaten) sowie von Verrechnungsdaten notwendig.

- **Entbündelung** bezeichnet eine Zugangsverpflichtung, die marktbeherrschenden Unternehmen mit beträchtlicher Marktmacht nach § 37 Abs 2, § 41 Abs. 2 Z 1 TKG 2003 auferlegt werden kann und in deren Rahmen Leitungssegmente des festen Kommunikationsnetzes eines Unternehmens mit beträchtlicher Marktmacht, die von der Vermittlungsstelle zum Teilnehmer führen (oder bestimmte Teilabschnitte davon), anderen Betreibern entweder physisch oder virtuell gegen Entgelt zur Verfügung zu stellen sind.
  Die Entbündelung als Zugangsverpflichtung wurde von der Regulierungsbehörde angeordnet und ist als Standardangebot in Form des Vertrags betreffend den Zugang zur Teilnehmeranschlussleitung sowie des Vertrags betreffend virtuelle Entbündelung am Markt verfügbar.
  In der Abwicklung bestehen jeweils grundsätzlich zwei ge-

trennte Vertragsverhältnisse: eines zwischen dem zugangsverpflichteten Betreiber und dem Nachfrager sowie eines zwischen dem Nachfrager und seinem Endkunden. Für die Durchführung der vertraglichen Beziehung zwischen Betreiber und Nachfrager (zB Herstellung, Entstörung) gemäß dem jeweiligen Standardangebot ist die Verarbeitung der Stammdaten des Nachfragers, die Verarbeitung der vom Nachfrager zur Verfügung gestellten Endkundenkontaktinformationen und der standortbezogenen Daten des Endkunden notwendig.

- **Mobile Virtual Network Operators (MVNOs)** sind Mobilfunkbetreiber welche über keine eigene Funkinfrastruktur verfügen, jedoch aufgrund eines Kooperationsvertrags mit einem Mobilfunknetzbetreiber Kommunikationsdienste über dessen Infrastruktur anbieten können. Betreibern von Mobilfunknetzen mit beträchtlicher Marktmacht können dabei von der Regulierungsbehörde gemäß § 41 TKG entsprechende Zugangsverpflichtungen auferlegt werden. Die Diensterbringung des MVNO im Netz des verpflichteten Betreibers erfolgt wie im Rahmen von National Roaming mithilfe der MSISDN, der Mobile Subscriber Integrated Services Digital Network Number. Zusätzlich werden dem Betreiber auch Standortdaten der Endkunden des MVNO übermittelt. Daten, welche eine direkte Identifizierung des Betroffenen ermöglichen würden werden nicht übermittelt.

II. Recht auf Auskunft

1. Im Sinne einer transparenten Datenverarbeitung werden die unterzeichnenden ISPs, ihren Kundinnen und Kunden einen Einblick in die sie betreffenden Datenverarbeitungsvorgänge geben, unterliegen jedoch bestimmten Einschränkungen aufgrund von sektorspezifischen Spezialbestimmungen.

2. Die Bereitstellung und Übermittlung von Verkehrsdaten erfolgt ausschließlich auf Grundlage der Spezialnormen des Materiengesetzes. Demnach dürfen Verkehrsdaten gemäß § 99 TKG vom ISP außer in den darin geregelten Fällen nicht gespeichert oder übermittelt werden. Dem Recht auf Auskunft nach gespeicherten Verkehrsdaten wird daher ausschließlich durch die Übermittlung des Einzelgesprächsnachweises gemäß § 101 TKG an den Kunden entsprochen.

3. Die unterzeichnenden Unternehmen können im Rahmen der Beauskunftung unter Berufung auf Artikel 15 Abs 1 lit c) Empfänger oder Kategorien von Empfängern von personenbezogenen Daten beauskunften. Letzteres kann insbesondere dann vonnöten sein, wenn es sich um Empfänger handelt, welche bei der technischen Durchführung des Kommunikationsdienstes tätig sind. Einer Beauskunftung über sämtliche konkrete Empfänger – insbesondere in dem genannten Bereich – können gewichtigen Sicherheitsbedenken entgegenstehen. Grund hierfür ist, dass es durch eine entsprechende Auskunft Kriminellen leicht möglich wäre, potentielle Schwachstellen zu identifizieren, um sich Zugriff auf das Netzwerk zu verschaffen. Hierdurch kann die Integrität des Systems, zu dessen Gewährleistung der Betreiber gemäß § 16a TKG verpflichtet ist, betroffen bzw. sogar gefährdet werden.

4. Jedenfalls nicht erfasst sind Informationen über Datenübermittlungen an Behörden im Rahmen ihrer Aufsichtsfunktion sowie an Strafverfolgungsbehörden, welche Daten etwa im Rahmen einer Inhaltsüberwachung übermittelt werden müssen.

5. Sofern der Betroffene das Auskunftsersuchen elektronisch einbringt, stellt der ISP auf Anfrage die Informationen ebenfalls in einem elektronischen Format zur Verfügung. Die unterzeichnenden Unternehmen treffen dabei entsprechende Datensicherheitsvorkehrungen um eine sichere Übertragung der Daten an den Betroffenen zu gewährleisten. Die Bereitstellung der Informationen in Papierform erfolgt mittels eingeschriebenen Briefs.

6. Um zu gewährleisten, dass die tatsächlich berechtigte betroffene Person die angefragten Daten erhält, führen die unterzeichnenden Unternehmen eine Identitätsüberprüfung durch.

III. Recht auf Einschränkung der Verarbeitung

1. Das Recht auf Einschränkung der Verarbeitung von personenbezogenen Daten soll grundsätzlich einem vorläufigen Ausgleich zwischen dem Interesse des Betroffenen an seinen personenbezogenen Daten und dem Interesse des Verantwortlichen an der Verarbeitung dieser Daten dienen. Der Betroffene kann dabei unter anderem vom Verantwortlichen verlangen, Daten vorerst nicht weiterzuverarbeiten – und damit auch nicht zu löschen – da er diese zur Geltendmachung oder Ausübung von bzw. zur Verteidigung gegen Rechtsansprüche benötigt.

2. Sofern der Betroffene in Ausübung dieses Rechts den ISP dazu auffordert, Verkehrsdaten nicht weiter zu verarbeiten bzw. nicht zu löschen, steht diesem Recht § 99 TKG entgegen, welcher für ISPs als lex specialis gilt. Verkehrsdaten dürfen demnach ausschließlich in den im TKG geregelten Fällen verarbeitet werden. Nach Beendigung der Verbindung sowie Begleichung der Rechnung hat der ISP die Verkehrsdaten zu löschen oder zu anonymisieren. Aufgrund dieser Verpflichtung ist es den unterzeichnenden ISPs somit rechtlich nicht erlaubt, Verkehrsdaten aufgrund von Geltendmachung des Rechts auf Einschränkung der Verarbeitung für einen darüberhinausgehenden Zeitraum aufzubewahren.

3. Gemäß § 100 Abs. 3 TKG sowie der Judikatur der Datenschutzbehörde werden dem Kunden Verkehrsdaten ausschließlich als verkürzter Einzelgesprächsnachweis zur Verfügung gestellt, außer der Teilnehmer hat schriftlich erklärt, dass er alle bestehenden Mitbenutzer des Anschlusses darüber informiert hat bzw. künftige Mitbenutzer informieren wird, dass er einen unverkürzten EGN erhält. Eine darüberhinausgehende Speicherung von passiven Teilnehmernummern oder sonstigen Angaben zur Identifizierung eines Empfängers einer Nachricht zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen kann vom Betroffenen daher nicht verlangt werden.

4. Inhaltsdaten dürfen vom ISP gemäß § 101 TKG nicht gespeichert werden, eine Einschränkung der Verarbeitung ist sohin nicht möglich.

5. Um zu gewährleisten, dass es sich bei der anfragenden Person tatsächlich um den Betroffenen handelt, führen die unterzeichnenden ISPs eine Identitätsüberprüfung durch.

   Sonderfall: Einschränkung von Daten in Backups anstelle Recht auf Löschung

6. Das Recht auf Löschung in Art 17 DSGVO dient Betroffenen grundsätzlich dazu, dass sie betreffende personenbezogene Daten auf Anfrage unverzüglich gelöscht werden, und verpflichtet den Verantwortlichen, personenbezogene Daten unverzüglich zu löschen, sofern keine vertragliche oder gesetzliche Verpflichtung oder Berechtigung für die Verarbeitung mehr vorliegt.

7. Löschungen aus Backup- oder Archivablagen stellen ISPs jedoch vor Herausforderungen, da es sich hierbei um gänzlich automationsunterstütze Vorgänge handelt und manuelle Eingriffe in den Löschzyklus zumeist nur mit hohem wirtschaftlichem und technischem Aufwand möglich sind, weshalb eine unverzügliche Löschung nicht möglich ist.

8. Da es noch keine gesicherten Rechtsmeinungen bzw. Judikatur zu Thema Datenverarbeitung gemäß DSGVO in Backups gibt, bleibt es jedem ISP überlassen, für eine möglichst DSGVO konforme Lösung von Datenverarbeitung in Backups zu sorgen. Eine Möglichkeit dabei kann folgende sein: Um die Interessen der Betroffenen jedoch gleichsam zu wahren wird die Verarbeitung der betreffenden personenbezogenen Daten daher eingeschränkt, bis der dokumentierte Backup- oder Archiv-Zyklus zur endgültigen Löschung führt. Das bedeutet, dass die betreffenden personenbezogenen Daten aus den primären Verarbeitungs-Systemen entfernt und dort nicht mehr verarbeitet werden.

IV. Recht auf Datenübertragbarkeit

1. Die unterzeichnenden Unternehmen verstehen das Recht auf Datenübertragbarkeit ausschließlich in Bezug auf personenbezogene Daten, die direkt vom Betroffenen auf Grundlage eines bestehenden Vertragsverhältnisses oder aufgrund von rechtmäßiger Einwilligung bereitgestellt wurden und sofern die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

2. Ziel ist es, den Kundinnen und Kunden die reibungslose Mitnahme der sie betreffenden personenbezogenen Daten zu ermöglichen. Die unterzeichnenden Unternehmen stellen dem Betroffenen daher die von diesem im Rahmen der Nutzung einer ISP-Dienstleistung bereitgestellten personenbezogenen Daten zur Verfügung.

3. Die unterzeichnenden Unternehmen erfüllen den Anspruch auf Datenübertragbarkeit durch die Bereitstellung der folgenden personenbezogenen Daten wie insbesondere:

   a) Stammdaten gemäß § 92 Abs. 3 Z 3 TKG , die vom Betroffenen bei der Anmeldung bzw. während des aufrechten Vertragsverhältnisses bereitgestellt werden:
      1) Name (Familienname und Vorname),
      2) akademischer Grad,
      3) Anschrift (Wohnadresse)
      4) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht

   Bonitätsdaten, Informationen zu Art und Inhalt des Vertragsverhältnisses sowie Profiling-Daten sind vom Anspruch auf Datenübertragbarkeit nicht umfasst, da diese nicht vom Betroffenen bereitgestellt werden und die Interpretation der Bonitätsprüfung jedem Verantwortlichen überlassen bleiben muss, um einen fairen Wettbewerb zu gewährleisten.

   b) Sonstige Daten welche vom Betroffenen bereitgestellt werden wie insbesondere:
      1) Geburtsdatum
      2) E-Mail-Adresse, die der Betroffene bekannt gegeben hat
      3) Inhalte des E-Mail-Postfachs (wenn der Verantwortliche selbst E-Mail Service – Betreiber dieses Postfaches ist)
      4) Bankverbindungsdaten

4. Im Sinne der Rechtsstaatlichkeit wird vom Recht auf Datenübertragbarkeit jedenfalls ausgeschlossen, dass Verkehrsdaten oder unverkürzte Einzelgesprächsnachweise (EGN) übertragen werden, da diese nicht vom Betroffenen bereitgestellt werden, Datenschutzrechte von Dritten unmittelbar berührt werden und Verkehrsdaten zudem gemäß § 99 TKG vom ISP außer in den darin geregelten Fällen nicht gespeichert oder übermittelt werden dürfen.
   Eine Übermittlung von gespeicherten Verkehrsdaten an Kundinnen und Kunden ist ausschließlich im Rahmen des Einzelgesprächsnachweises (§ 100 TKG) erlaubt. Gemäß der Rechtsprechung der DSB, werden darüber hinaus keine Verkehrsdaten an den Kunden bzw. die Kundin beauskunftet und somit auch nicht portiert.

Bereitstellung der Daten an den Betroffenen

5. Die unterzeichnenden Unternehmen stellen dem Betroffenen die ihn betreffenden personenbezogenen Daten, die dieser direkt, aufgrund einer rechtmäßigen Einwilligung oder im Rahmen eines Vertragsverhältnisses zur Verfügung gestellt hat, in elektronischer Form (z.B. als Download oder Übermittlung per E-Mail) bereit.

6. Um die Bereitstellung via Download zu ermöglichen wird dem Betroffenen entweder ein Downloadlink übermittelt oder ein Downloadbutton im Kundenbereich der Unternehmenswebseite eingerichtet.

7. Daten, welche vom Betroffenen selbst ohne Aufwand jederzeit in einem gängigen, maschinenlesbaren Format bezogen werden können, gelten als bereitgestellt.

8. Die unterzeichnenden Unternehmen unterlassen jegliche technischen Maßnahmen welche eine nachträgliche Übermittlung der erhaltenen Daten durch den Betroffenen an einen neuen Verantwortlichen erschweren.

Dateiformat

9. Stammdaten des Betroffenen iSv Pkt. 3 a) 1 - 4 sowie Geburtsdatum, E-Mail-Adresse und Bankverbindungsdaten werden von den unterzeichnenden Unternehmen gesammelt als Textdatei in einem gängigen Format z.B. im Format XML, CSV oder XLS bereitgestellt.

10. Der Inhalt des E-Mail-Postfachs wird in einem gängigen Format wie z.B. MBOX-Datei-Format oder durch Abrufbarkeit über IMAP, POP oder ActiveSync im Postfach bereitgestellt.

11. Es liegt im Ermessen des Betreibers, ob er einzelne Daten- oder Datenkategorien bzw. alle Daten gesammelt in einer Datei (z.B. ZIP-Datei) als Archiv portiert.

Übermittlung der Daten an einen neuen Verantwortlichen

12. Auf Wunsch des Betroffenen stellen die unterzeichnenden Unternehmen – soweit nicht anders angeführt – die erfassten Daten dem neuen Verantwortlichen auf die gleiche Art und Weise zur Verfügung wie dem Betroffenen.

13. Um die Implementierung der bereitgestellten Daten durch einen neuen Verantwortlichen sicherzustellen bedarf es gemeinsamer technischer Standards innerhalb der ISP-Branche auf europäischer Ebene. Bis dahin ist die Weiterverwendbarkeit der Daten durch den neuen Verantwortlichen möglicherweise nicht gewährleistet.

V. Identitätsnachweis

Um zu gewährleisten, dass die tatsächlich berechtigte betroffene Person ihre Betroffenenrechte gemäß DSGVO ausübt, können die unterzeichnenden Unternehmen Identitätsüberprüfungen durchführen.

VI. Data-Breach-Notification

1. Im Falle eines Sicherheitsvorfalls der zu einer Verletzung des Schutzes personenbezogener Daten führt, übermitteln die unterzeichnenden Unternehmen unverzüglich, spätestens jedoch innerhalb von 24h , eine Benachrichtigung an die Datenschutzbehörde (Data Breach Notification).

2. Die unterzeichnenden ISPs erfüllen im Rahmen der Data Breach Notification die formellen und inhaltlichen Anforderungen an die Meldung welche im Musterformular (Anhang A) näher definiert sind.

3. Unterlässt der ISP eine Benachrichtigung so wird er die Gründe im Rahmen seiner Dokumentationspflicht festhalten.

Benachrichtigung des Betroffenen

4. Sofern die Verletzung des Schutzes personenbezogener Daten mit hoher Wahrscheinlichkeit zu einem materiellen oder immateriellen Schaden des Betroffenen führt, übermittelt der ISP zusätzlich zu Pkt 1. eine Benachrichtigung an den Betroffenen. Je höher der potentiell eintretende Schaden ist, desto geringer ist die notwendige Eintrittswahrscheinlichkeit, um eine Benachrichtigung auszulösen.

5. Da vom ISP nur der eigene Vertragskunde kontaktiert werden kann, nicht jedoch etwaige Gesprächspartner, welche von einem Data-Breach ebenso betroffen sein könnten, ist es den unterzeichnenden ISPs nur möglich, eine Data-Breach-Notification an den jeweiligen Vertragskunden durchzuführen. Sofern von dem Data-Breach eine hohe Anzahl an Nicht-Vertragskunden betroffen ist, wird der ISP diese mittels öffentlicher Bekanntmachung des Data-Breaches informieren.

Bemessungskriterien

6. Die unterzeichnenden ISPs bemessen die drohende Schadensschwere sowie dessen Eintrittswahrscheinlichkeit jeweils im Einzelfall anhand der Art des Sicherheitsvorfalls, der Kategorien der betroffenen Daten sowie der sich daraus ergebenden Missbrauchsmöglichkeiten durch Dritte.

7. Insbesondere wird dabei berücksichtigt ob eines der folgenden Szenarios droht:

    a. Verlust der Kontrolle über die Daten,
    b. Diskriminierung,
    c. Identitätsdiebstahl oder -betrug,
    d. finanzielle Verluste,
    e. unbefugte Aufhebung der Pseudonymisierung,
    f. Rufschädigung
    g. Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten

8. Durch technische und organisatorische Maßnahmen, die der ISP in Bezug auf die betroffenen personenbezogenen Daten ergriffen hat oder ergreifen wird, kann die Eintrittswahrscheinlichkeit entsprechend gesenkt werden.

9. Ein hohes Risiko für materielle und immaterielle Schäden beim Betroffenen wird von den unterzeichnenden Unternehmen insbesondere dann angenommen, wenn unverkürzte Kreditkartennummern, Passwörter oder Kommunikationsinhalte betroffen sind.

VII. Teilnahme an den Verhaltensregeln

1. Internet Service Provider, welche in den räumlichen und sachlichen Geltungsbereich dieser Verhaltensregeln fallen, können sich diesen Verhaltensregeln unterwerfen und geben dies per E-Mail an aufsichtsbeirat_coc@ispa.at oder per Post an Währinger Straße 3/18, 1090 Wien bekannt.

2. Liegen die Voraussetzungen gemäß Punkt 1 nicht vor, wird der betroffener Anwerber nicht in die Liste der unterzeichnenden Unternehmen aufgenommen.

3. Auf der Webseite der ISPA wird eine aktuelle Liste mit allen Unternehmen, welche den Code of Conduct unterzeichnet haben, veröffentlicht. Diese Liste enthält den Namen und die Adresse des unterzeichnenden Unternehmens.

4. Die unterzeichnenden Unternehmen haben einen Link zu der aktuellen Liste mit den unterzeichnenden Unternehmen auf ihre Webseite zu setzen.

VIII. Überwachung der Einhaltung der Verhaltensregeln

1. Ein Aufsichtsbeirat wird in Form einer Organisationseinheit innerhalb der ISPA als das zuständige Organ zur Überwachung der Einhaltung der vorliegenden Verhaltensregeln gemäß Artikel 41 DSGVO eingerichtet.

2. Jedes diese Verhaltensregeln unterzeichnende Unternehmen, verpflichtet sich zur Anerkennung der Empfehlungen und Entscheidungen dieses Aufsichtsbeirates.

3. Die genauen Kriterien zur Bestellung der Mitglieder des Aufsichtsbeirats sowie zu dessen Tätigkeit werden in einer separaten Geschäftsordnung festgelegt. Diese kann unter www.ispa.at/coc abgerufen werden.

Anhang A

I. Musterformular für eine Benachrichtigung der Datenschutzbehörde über eine Verletzung des Schutzes personenbezogener Daten

(Alle Angaben sollten möglichst in der Erstbenachrichtigung an die Behörde enthalten sein, welche unverzüglich, jedenfalls jedoch innerhalb von 24 Stunden ab Feststellung des Vorfalls erfolgen muss)

Anmerkung: Dieses Formular entspricht dem ANHANG I der Verordnung (EU) Nr. 611/2013 der Kommission vom 24. Juni 2013 über die Maßnahmen für die Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten gemäß der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates (Datenschutzrichtlinie für elektronische Kommunikation) sowie den Anforderungen des § 95a TKG. Dieses Formular berücksichtigt auch die inhaltlichen Mindestanforderungen an die Meldung nach Art 33 Verordnung (EU) 2016/679 (Datenschutzgrundverordnung).

Angaben zum Betreiber

1. Name und Kontaktdaten eines oder mehrerer informierter Ansprechpartner für allfällige Rückfragen

Name: _____ Position: _____

Telefonnummer: _____ E-Mailadresse: _____

2. Angabe, ob es sich um eine Erstbenachrichtigung oder eine Folgebenachrichtigung handelt

☐ Erstbenachrichtigung ☐ Zweite oder Folgebenachrichtigung

3. Datum und Zeitpunkt des Vorfalls (falls bekannt, kann nötigenfalls geschätzt werden) und der Feststellung des Vorfalls

Datum und Zeitpunkt des Vorfalls: _____ Datum und Zeitpunkt der Feststellung des Vorfalls: _____

4. Art der Verletzung des Schutzes personenbezogener Daten

Vernichtung, Verlust, Beschädigung, unbefugte Offenlegung

- ☐ Vernichtung: Die Daten sind nicht mehr verfügbar/wurden gelöscht
- ☐ Verlust: Die Daten existieren zwar noch, aber der Verantwortliche hat die Kontrolle/Zugriff/Besitz verloren
- ☐ Beschädigung: Die Daten wurden verändert, beschädigt oder sind nicht mehr vollständig
- ☐ Unbefugte Offenlegung: Weitergabe der Daten an Empfänger, die nicht berechtigt sind, die Daten zu empfangen (oder darauf zuzugreifen)

5. Art und Inhalt der betroffenen personenbezogenen Datensätze

Angabe der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze (insbes. ob es sich um besondere personenbezogene Daten, Daten über strafrechtliche Verurteilungen, biometrische Daten oder Gesundheitsdaten handelt)

6. Kategorien und Anzahl der betroffenen Personen
Angabe der nach Typisierungsangaben abstrakt zusammengefassten potentiell betroffenen Gruppen („Beschäftigte“, „Kundinnen und Kunden“...)

Sofern eine Angabe der Anzahl nicht möglich ist, eine Begründung warum eine Abschätzung der Anzahl der betroffenen Teilnehmer oder Personen zum Zeitpunkt der Meldung nicht möglich ist.

7. Technische und organisatorische Maßnahmen, die der Betreiber in Bezug auf die betroffenen personenbezogenen Daten ergriffen hat (oder ergreifen wird)

Technische und organisatorische Maßnahmen um die eingetretene Verletzung zu beseitigen sowie ggf. die nachteiligen Auswirkungen zu minimieren
z.B. Zurücksetzung der Passwörter, Zugangssperren, bei strafbaren Handlungen Anzeige bei der zuständigen Polizeidienststelle

8. Mögliche Folgen und mögliche nachteilige Auswirkungen auf Teilnehmer oder Personen
Angaben über die potentiellen materiellen oder immateriellen Schäden, wie etwa Verlust der Kontrolle über die personenbezogenen Daten, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung oder der Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten

II. Musterformular für eine Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(Die Angaben haben in klarer und verständlicher Sprache zu erfolgen)

Anmerkung: Dieses Formular entspricht den inhaltlichen Mindestanforderungen an die Meldung nach Art 34 Verordnung (EU) 2016/679 (Datenschutzgrundverordnung).

Ausnahmen von der Benachrichtigungspflicht (Unterlässt der Betreiber eine Benachrichtigung so hat er die Gründe im Rahmen der Dokumentationspflicht festzuhalten)

1.) Vorliegen von technischen und organisatorischen Sicherheitsvorkehrungen die geeignet sind, dass die personenbezogenen Daten unbefugten Personen unzugänglich sind (Verschlüsselung, Pseudonymisierung)
2.) Im Anschluss an die Datenschutzverletzung ergriffene Maßnahmen welche das ursprünglich hohe Risiko eines Schadens beseitigen
3.) Die Benachrichtigung ist mit unverhältnismäßigem Aufwand verbunden (in diesem Fall hat nur eine öffentliche Bekanntmachung zu erfolgen)

Angaben zum Betreiber

1. Name und Kontaktdaten eines oder mehrerer informierter Ansprechpartner für allfällige Rückfragen

Name: _____ Position: _____

Telefonnummer: _____ E-Mailadresse: _____

2. Datum und Zeitpunkt des Vorfalls (falls bekannt, kann nötigenfalls geschätzt werden) und der Feststellung des Vorfalls

Datum und
Zeitpunkt des Vorfalls: _____

Datum und Zeitpunkt
der Feststellung des Vorfalls: _____

3. Art der Verletzung des Schutzes personenbezogener Daten

Vernichtung, Verlust, Veränderung, unbefugte Offenlegung

- ☐ Vernichtung: Die Daten sind nicht mehr verfügbar/wurden gelöscht
- ☐ Verlust: Die Daten existieren zwar noch, aber der Verantwortliche hat die Kontrolle/Zugriff/Besitz verloren
- ☐ Beschädigung: Die Daten wurden verändert, beschädigt oder sind nicht mehr vollständig
- ☐ Unbefugte Offenlegung: Weitergabe der Daten an Empfänger, die nicht berechtigt sind, die Daten zu empfangen (oder darauf zuzugreifen)

4. Technische und organisatorische Maßnahmen, die der Betreiber in Bezug auf die betroffenen personenbezogenen Daten ergriffen hat (oder ergreifen wird)

Technische und organisatorische Maßnahmen um die eingetretene Verletzung zu beseitigen sowie ggf. die nachteiligen Auswirkungen zu minimieren
z.B. Zurücksetzung der Passwörter, Zugangssperren, bei strafbaren Handlungen Anzeige bei der zuständigen Polizeidienststelle

5. Mögliche Folgen und mögliche nachteilige Auswirkungen für den Betroffenen

Angaben über die potentiellen materiellen oder immateriellen Schäden, wie etwa Verlust der Kontrolle über die personenbezogenen Daten, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung oder der Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten

Version

Version 1.1. v. 16.06.2020

Über ISPA

Die ISPA – Internet Service Providers Austria ist der Dachverband der österreichischen Internetwirtschaft. Sie wurde 1997 als eingetragener Verein gegründet und vertritt rund 220 Mitglieder aus den Bereichen Access, Content und Services u. a. gegenüber Politik, Verwaltung und anderen Gremien. Ziel der ISPA ist die Förderung des Internets sowie die Kommunikation der Marktteilnehmer untereinander.

@ispa_at
www.facebook.com/ispa.internetserviceprovidersaustria

ISPA – Internet Service Providers Austria
Währinger Straße 3/18, 1090 Wien, Austria
☎ +43 1 409 55 76
✉ office@ispa.at
www.ispa.at

EU-Transparenzregister: 56028372438-43
LIV-Register: LIVR-00226