Hinweise für Verbraucher gemäß § 43a Abs. 1 Nr. 12 TKG sowie Abs. 2 Nr. 4 TKG über Verfahren zur Vermeidung von Aus- und Überlastungen sowie zur Reaktion auf Sicherheits- oder Integritätsverletzungen, Bedrohungen und Schwachstellen

I. Informationen über die von Tele2 zur Messung und Kontrolle des Datenverkehrs eingerichteten Verfahren zur Vermeidung einer Kapazitätsauslastung oder Überlastung einer Netzwerkverbindung sowie Informationen über die möglichen Auswirkungen dieser Verfahren auf die Dienstqualität

Soweit Plattformen, Netzelemente und Systeme zur Abwicklung des Datenverkehrs von Mobilfunk- und Festnetzprodukten von Tele2 selbst betrieben werden, werden diese – im Rahmen der technischen Möglichkeiten – gemessen und kontrolliert. Diese Überwachung erfolgt automatisch und liegt im Verantwortungsbereich des Network Operation Centers (NOC) unter Zuhilfenahme marktüblicher Netzwerküberwachungssysteme. Die eingesetzten Überwachungssysteme liefern regelmäßige Informationen zur Auslastung und Performance der beteiligten Netzelemente und Übertragungsstrecken. Anhand dieser Informationen kann Tele2 im Bedarfsfall geeignete Maßnahmen zur Vermeidung einer Kapazitätsauslastung oder Überlastung einer Netzwerkverbindung einleiten, wie etwa durch ein Ausweichen auf andere Systeme oder alternative Übertragungsstrecken. Zudem werden rechtzeitig notwendige Kapazitätserweiterungen vorgenommen um die übliche Dienstqualität der von Tele2 vertriebenen Produkte sicher zu stellen.

Soweit Plattformen, Netzelemente und Systeme zur Abwicklung des Datenverkehrs von Mobilfunk- und Festnetzprodukten von Dritten betrieben werden, wurden mit diesen Unternehmen Service-Level-Agreements vereinbart, die eine den von Tele2 vertriebenen Produkten entsprechende Dienstqualität des von diesem Drittunternehmen abgewickelten Datenverkehrs sicher stellen sollen. Um die Einhaltung dieser Service-Level-Agreements gewährleisten zu können, wurden die Drittunternehmen von Tele2 verpflichtet, durch geeignete technische und organisatorische Maßnahmen sicher zu stellen, dass die in den vereinbarten Service-Level-Agreements verankerte Dienstqualität erfüllt wird.

II. Maßnahmen zur Reaktion auf Sicherheits- oder Integritätsverletzungen sowie Bedrohungen und Schwachstellen

Tele2 nimmt die Gewährleistung der Sicherheit der bereitgestellten Dienste sehr ernst und hat strukturelle Maßnahmen ergriffen, durch die Tele2 sowohl präventiv Schwachstellen entgegen wirken, als auch im konkreten Fall einer Sicherheits- oder Integritätsverletzung erforderliche Schritte einleiten kann.

1. Präventive Maßnahmen und Organisation

a) Tele2 hat einen internen Sicherheitsbeauftragten bestellt, der die Verantwortung dafür trägt, Sicherheitsrisiken zu erkennen, die den Geschäftsbetrieb von Tele2 gefährden. Im Fokus dieser Sicherheitsanalyse steht der Schutz der von Tele2 betriebenen Telekommunikations- und IT-Infrastruktur. Dazu gehört insbesondere die Sicherstellung geeigneter Maßnahmen zur Abwehr etwaiger Bedrohungen durch Eindringen unbefugter Dritter in die Geschäftsräume oder Angriffe auf die technischen Einrichtungen von Tele2.

b) Über den von Tele2 Deutschland bestellten Sicherheitsbeauftragten hinaus gibt es in der Muttergesellschaft Tele2 AB eine zentrale Abteilung „Konzernsicherheit“. Diese wird von dem zentralen Sicherheitsbeauftragen der Tele2-Gruppe geleitet. Dieser beaufsichtigt die internen Sicherheitsbeauftragten in den einzelnen Tele2-Landesgesellschaften und stellt sicher, dass in allen Tele2-Landesgesellschaften die gleichen Sicherheitsstandards und –prozesse angewendet werden. Die konzernweit einheitlich getroffenen Regelungen und Standards zur Vermeidung von Sicherheitsrisiken werden in einem Sicherheitshandbuch dokumentiert, für deren Umsetzung der interne Sicherheitsbeauftragte und die

Geschäftsführung in der jeweiligen Landesgesellschaft verantwortlich sind. Um einen regelmäßigen Austausch zwischen den internen Sicherheitsbeauftragten der Landesgesellschaften und dem zentralen Sicherheitsbeauftragten zu ermöglichen, findet mindestens einmal jährlich ein Treffen mit den internen Sicherheitsbeauftragten der Landesgesellschaften und dem zentralen Sicherheitsbeauftragten statt.

c) Der zentrale Sicherheitsbeauftragte initiiert in unregelmäßigen Abständen Audits mit dem Ziel der Überprüfung, inwieweit die im Sicherheitshandbuch dokumentierten Standards von der jeweiligen Landesgesellschaft eingehalten werden.

2. Reaktionen auf Sicherheits- oder Integritätsverletzungen

a) Der interne Sicherheitsbeauftragte der jeweiligen Landesgesellschaft ist dazu verpflichtet sämtliche Vorfälle bei denen es zu Sicherheits- und Integritätsverletzungen gekommen ist, unverzüglich der Geschäftsführung der Landesgesellschaft sowie dem zentralen Sicherheitsbeauftragten zu melden.

b) Im Falle eines sicherheitsrelevanten Vorfalles initiiert der zentrale Sicherheitsbeauftrage eine Untersuchung, welche Ursachen zu dem jeweiligen Ereignis geführt haben und mit welchen Maßnahmen zu reagieren ist um einen eventuell eingetreten Schaden zu beseitigen sowie um ähnliche Vorfälle in Zukunft zu vermeiden.

c) Der lokale Sicherheitsbeauftragte ist außerdem für die Hinterlegung eines aktuellen Sicherheitskonzeptes bei der Bundesnetzagentur verantwortlich, das die getroffenen Maßnahmen gegenüber der zuständigen Regulierungsbehörde dokumentiert.

d) Für die Sicherstellung der Integrität der Kundendaten hat Tele2 einen separaten Datenschutzbeauftragten bestellt, der die Einhaltung sämtlicher datenschutzrechtlichen Bestimmungen überwacht.