Technical and organisational measures (toMs) to be implemented by the supplier when processing personal data on behalf of Vodafone

1 Entrance control

1.1 Entrances to the premises of Processor where VF Data is processed must be protected against unauthorised access by security or swipe card locks.

1.2 Doors, gates and windows of the premises of Processor where VF Data is processed must be kept locked out of working hours; doors, gates and windows in the basement and on the ground floor as well as all other easily accessible entrances to these rooms must be constructed so that unauthorised access is rendered considerably more difficult, for example by using anti-burglary doors, gates, windows and locks or by installation of an intruder alarm.

1.3 Servers used by Processor to execute this DPA must be kept in a separate, secured server room or computer centre, which must be separately protected against unauthorised access by an access control system complying with the current state of the art in security technology. These rooms are constructed burglar resistant. Access to these rooms shall be limited to maintenance and repair as well as to the specifically required functions and persons. Access to these rooms shall be recorded immediately after accessing the rooms and for a period of 90 days after-wards each. Processor shall conduct at least randomised sample inspections of these records at regular intervals.

1.4 Granting access authorisations and issuance of keys, swipe cards, badges and other means of identification al-lowing for access shall be documented in a trackable manner in form of an up-to-date list of means of unlocking and access authorisations for the duration of the Master Agreement.

2 Admission control

2.1 The information processing systems (client and server systems) utilised by Processor for execution of this DPA are protected by authentication and authorisation systems.

2.2 Identification and authentication information (especially in form of usernames and passwords) that are associated with the access authorisations to the information pro-cessing systems for execution of this DPA, shall only be given to the persons commissioned with the execution of this DPA and only to the extent required for the task in question.

2.3 Any disclosure of access authorisations is documented during the term of the Master Agreement.

2.4 All access points and identifications (“accounts”) shall exclusively be assigned to specific persons. The use of accounts by several persons (“group accounts”) does not take place as a matter of principle. If the use of group ac-counts cannot be avoided, it is ensured that the exact time of use of the group account by a specific natural per-son can be determined.

2.5 Identification and authentication information is exclusively used personally; it shall not be disclosed. Insofar as unauthorised people gain access to access information, Processor shall inform Vodafone thereof immediately.

Durch den Lieferanten umzusetzende technische und organisatorische Maßnahmen (toMs) bei der Verarbeitung personenbezogener Daten im Auftrag von Vodafone

1 Zutrittskontrolle

1.1 Die Eingänge zu den Räumlichkeiten des Auftragsverarbeiters, in denen VF-Daten verarbeitet werden, sind mit Sicherheits- oder Magnetkartenschlössern gegen Zutritt Unbefugter gesichert.

1.2 Türen, Tore und Fenster der Räumlichkeiten des Auftragsverarbeiters, in denen VF-Daten verarbeitet werden, sind außerhalb der Betriebszeiten fest verschlossen; Türen, Tore und Fenster in Keller und Erdgeschoss sowie alle weiteren leicht zu erreichenden Zugänge zu diesen Räumen sind derart ausgeführt, dass diese Unbefugten nur erheblich erschwert zugänglich sind, etwa durch ein-bruchhemmende Türen, Tore, Fenster und Schlösser o-der den Einsatz einer Einbruchmeldeanlage.

1.3 Zur Durchführung dieser AV vom Auftragsverarbeiter verwendete Server sind in einem separat abgesicherten Serverraum oder Rechenzentrum untergebracht, welche durch eine Zutrittskontrollanlage nach dem aktuellen Stand der Sicherheitstechnik gegen den Zutritt Unbefugter gesondert gesichert sind. Diese Räume sind ein-bruchhemmend geschützt. Der Zutritt zu diesen Räumlichkeiten ist auf das zur Wartung und Instandsetzung sowie auf die im Übrigen konkret erforderlichen Rollen und Personen beschränkt. Unverzüglich beim Betreten und für jeweils einen Zeitraum von 90 Tagen nach Betreten der Räumlichkeiten werden die Zutritte zu diesen Räumlichkeiten protokollieren. Der Auftragsverarbeiter prüft die Protokolle regelmäßig, zumindest stichproben-artig.

1.4 Die Vergabe von Zutrittsberechtigungen und von Schlüsseln, Magnetkarten, Ausweisen sowie anderen den Zutritt ermöglichenden Identitätsmerkmalträgern ist für die Laufzeit des Hauptvertrags nachvollziehbar in Form einer aktuellen Auflistung der ausgegebenen Schließmittel und Zutrittsberechtigungen dokumentiert.

2 Zugangskontrolle

2.1 Die zur Durchführung dieser AV vom Auftragsverarbeiter eingesetzten informationsverarbeitenden Systeme (Client- und Serversysteme) sind durch Authentifikations- und Autorisationssysteme geschützt.

2.2 Identifikations- und Authentifikationsinformationen (insbesondere in Form von Benutzernamen und Passwörtern), welche mit der Zugangsberechtigung zu den zur Durchführung dieser AV eingesetzten informationsverarbeitenden Systemen verbunden sind, werden nur an die mit der Durchführung dieser AV beauftragten Personen und lediglich in dem für die jeweilige Aufgabe erforderlichen Umfang vergeben.

2.3 Jede Vergabe von Zugangsberechtigungen wird für die Laufzeit des Hauptvertrags dokumentiert.

2.4 Alle Zugänge und Kennungen („Accounts“) werden ausschließlich personenspezifisch vergeben. Die Benutzung von Accounts durch mehrere Personen (Gruppen-Accounts) unterbleibt grundsätzlich. Ist die Benutzung von Gruppen-Accounts unvermeidbar, ist die zeitgenaue Zuordenbarkeit der Nutzung eines Gruppen-Accounts durch eine konkrete natürliche Person sichergestellt.

2.5 Identifikations- und Authentifikationsinformationen wer-den ausschließlich persönlich verwendet, jegliche Weitergabe unterbleibt. Sofern Unbefugte Kenntnis von Zugangsdaten erhalten, zeigt der Auftragsverarbeiter dies Vodafone unverzüglich an.

2.6 Passwords shall be selected subject to sufficient complexity and quality. Sufficient complexity and quality means a length of at least eight (8) characters using three of the following four categories (uppercase and lower-case letters, numbers and special characters), no use of generic terms or own names as well as inadmissibility of at least the three (3) most recent passwords. Passwords must be changed after three (3) months at the latest.

2.6 Die Wahl der Passwörter erfolgt in ausreichender Komplexität und Güte. Ausreichende Komplexität und Güte bedeutet mindestens eine Länge von acht (8) Zeichen bei Nutzung von drei der folgenden 4 Kategorien (Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen), keine Verwendung generischer Begriffe oder von Eigennamen sowie die Unzulässigkeit mindestens der letzten drei (3) verwendeten Passwörter. Passwörter werden spätestens alle drei (3) Monate geändert.

2.7 Processor shall maintain strict secrecy concerning authentication information (especially passwords and cryptographic keys) towards unauthorised persons, shall not store these in plain text and shall use these exclusively subject to application of any of the encryptions or irreversible cryptographic checksums in accordance with clause 8 (especially in case of storage and transmission in a network).

2.7 Der Auftragsverarbeiter hält Authentifikationsdaten (insbesondere Passwörter und kryptographische Schlüssel) gegenüber Unbefugten streng geheim, bewahrt diese nicht im Klartext auf und verwendet diese ausschließlich unter Einsatz einer Ziffer 8 entsprechenden Verschlüsselung oder als unumkehrbare kryptographische Prüfsumme (insbesondere bei der Speicherung und der Übertragung im Netzwerk).

3 Access control

3.1 Where VF Data are stored in systems for information processing in order to execute this DPA, a graduated and suitable granular rights system is established and technically implemented for any and all access to VF Data. This ensures that the design of access rights is such that they only allow the respective employee charged with performance of the specific service to access the VF Data to the extent necessary. In this concept, assigning administrator rights is limited to the mandatory minimum of employees of Processor. Assignment of rights is documented for the duration of the Master Agreement.

3 Zugriffskontrolle

3.1 Sofern VF-Daten zur Durchführung dieser AV auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, ist für sämtliche Zugriffe auf VF-Daten ein abgestuftes und geeignet granulares Rechtesystem eingerichtet und technisch implementiert. Dadurch ist sichergestellt, dass die Zugriffsrechte so gestaltet sind, dass sie nur den für die Leistungserbringung eingesetzten Mitarbeiter jeweils für die Erfüllung der konkreten Aufgaben im notwendigen Umfang Zugriff auf die VF-Daten erlauben. Dabei ist die Vergabe von Administratorenrechte auf das zwingend erforderliche Maß an Mitarbeitern des Auftragsverarbeiters begrenzt. Die Rechte-vergabe wird für die Laufzeit des Hauptvertrags dokumentiert.

3.2 Insofar as VF Data is stored on systems for processing information of Processor, any and all access to VF Data (including modifying and deleting access) is recorded split by user, date, and time, at least for a duration of 90 days.

3.2 Sofern VF-Daten auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, werden sämtliche Zugriffe auf VF-Daten (einschließlich des verändernden und löschenden Zugriffs) nach Benutzer, Datum und Uhrzeit mindestens für die Dauer von 90 Tagen protokolliert.

3.3 Insofar as Processor collects and stores images of original documents with VF Data for performance of the services under the Master Agreement, the resulting image files shall be encrypted in accordance with clause 8. Where Processor has access to VF Data in form of recordings of conversations or other audio files, suitable measures are taken to prevent that the content stored therein is listened to or disclosed by uninvolved employees or other third parties.

3.3 Sofern der Auftragsverarbeiter zur Leistungserbringung nach dem Hauptvertrag Abbilder von Originaldokumenten mit VF-Daten elektronischer Form erfasst und speichert, werden die resultierenden Bilddateien dabei nach Maßgabe der Ziffer 8 verschlüsselt. Soweit der Auftragsverarbeiter Zugriff auf VF-Daten in Form von Gesprächsaufzeichnungen oder sonstigen Audio-Daten hat, wird durch geeignete Vorkehrungen verhindert, dass die dort gespeicherten Inhalte nicht von unbeteiligten Mitarbeitern oder sonstigen Dritten gehört oder wiedergegeben werden können.

4 Disclosure control

4.1 VF Data cannot be copied (especially not stored on external data carriers), disclosed and/or deleted without authorisation.

4 Weitergabekontrolle

4.1 VF-Daten können nicht unbefugt kopiert (insbesondere auf externe Datenträger gespeichert), weitergegeben und/oder gelöscht werden.

4.2 On the systems for data processing destined for end users (clients) used by Processor for execution of this DPA, the screensaver shall be activated after logging out of the system or after no more than fifteen (15) minutes of inactivity of the logged-in user.

4.2 Auf den vom Auftragsverarbeiter zur Durchführung dieser AV verwendeten informationsverarbeitenden Systemen für Endanwender (Clients) wird der Bildschirm-schoner bei Verlassen des Systems bzw. bei Inaktivität des angemeldeten Nutzers nach spätestens fünfzehn (15) Minuten aktiviert.

4.3 Data carriers as well as any and all documents, provided they contain VF Data (including any and all backup copies of VF Data and copies of original documents, where applicable) shall be kept in properly locked data protection cupboards used exclusively for the execution of this DPA, when and for as long as it is not being used.

4.3 Datenträger sowie sämtliche Dokumente, sofern sie VF-Daten enthalten (einschließlich sämtlicher gegebenenfalls vorhandener Sicherungskopien von VF-Daten und Kopien von Originaldokumenten) werden in ordnungsgemäß verschlossenen, und ausschließlich für die Durchführung dieser AV genutzten Datensicherungsschränken verwahrt, wenn und solange sie nicht in der Bearbeitung sind.

4.4 Documents containing VF DPA shall, also in the event of brief absence from the workstation, be protected against unauthorised access ("Clean Desk Policy").

4.4 Dokumente mit VF-Daten werden, auch bei auch nur kurzzeitigem Verlassen des Arbeitsplatzes, vor unberechtigtem Zugriff geschützt ("Clean Desk Policy").

4.5 Server systems with non-volatile memory used by the Processor in performance of this DPA, , e.g. network printers or scanner, shall not retain VF Data longer than as imminently required for contract performance.

5 Separation principle

Where VF Data is stored on systems for data processing of Processor, complete separation of the VF Data from personal data of other clients shall be implemented and it is thus guaranteed that the VF Data can at all times be fully identified and deleted, e.g. by storage of the VF Data in an own client, an own partition or in a container used for this purpose only. A corresponding separation shall also be realised for VF Data itself if it is stored for different purposes.

6 Availability control

6.1 The client systems (desktop and notebook computers) used by Processor for execution of the DPA run, where possible from a technical point of view, storage-resident virus scanners with at least one update per day as well as a personal firewall. Processor shall refrain from connecting these systems directly, i.e. without taking the security measures set out in the first sentence, with the Internet.

6.2 Server systems used by Processor to execute this DPA are protected by firewalls that protect these server systems against any access not required for operational rea-sons. These firewalls shall be operated on dedicated and hardened systems, i.e. systems limited to components, services and interfaces required for operation and shall be updated to new technical developments immediately. The firewalls work with a rule-based packet filter and ensure that the set of rules that is being used limits communication from and to the systems for data processing of Processor to the minimum required for operation of these systems by applying explicit authorisations ("White List"). Changes to the configuration of the firewall and/or the set of rules used are documented in permanent and trackable form (“tamper-proof”) for the duration of the Master Agreement.

6.3 Any and all software that may be used by Processor to execute this DPA shall be kept updated and security-relevant updates (especially patches, fixes) shall be in-stalled immediately after they were made available to the public by the software manufacturer and tested by Processor subject to a state-of-the-art procedure.

6.4 Original documents that contain VF Data as well as VF Data rightfully stored on systems for data processing by Processor shall be protected against loss due to accidental, negligent or intentional deletion or modification by taking technical and organisational measures.

6.5 Backup copies of VF Data rightfully stored on systems for data processing by Processor shall be treated subject to the same provisions as the original data, especially regarding protection against unauthorised access.

4.5 Auf zur Durchführung dieser AV vom Auftragsverarbeiter verwendeten Server-Systemen mit nichtflüchtigem Speicher, z.B. Netzwerkdrucker oder Scanner, werden VF-Daten nicht über den unmittelbar zur Vertragsdurchführung erforderlichen Umfang hinaus gespeichert.

5 Trennungsgebot

Sofern VF-Daten auf informationsverarbeitenden Systemen des Auftragsverarbeiters gespeichert sind, wird eine vollständige Trennung der VF-Daten von personenbezogenen Daten anderer Auftraggeber realisiert und dadurch die jederzeitige und vollständige Identifizier- und Löschbarkeit von VF-Daten sichergestellt, z.B. durch Speicherung der VF-Daten in einem eigenen Mandanten, in einer eigenen Partition oder in einem nur zu diesem Zweck verwendeten Container. Eine entsprechende Trennung wird auch für VF-Daten selbst realisiert, wenn sie zu verschiedenen Zwecken gespeichert werden.

6 Verfügbarkeitskontrolle

6.1 Auf den vom Auftragsverarbeiter zur Durchführung dieser AV verwendeten Client-Systemen (Desktops, Notebooks) laufen, soweit technisch möglich, speicherresidente Virenscanner mit mindestens täglichen Updates sowie eine Personal Firewall. Der Auftragsverarbeiter hat es zu unterlassen, diese Systeme direkt, d.h. ohne Einsatz der Sicherheitsmaßnahmen gemäß Satz 1 mit dem Internet zu verbinden.

6.2 Vom Auftragsverarbeiter zur Durchführung dieser AV verwendete Server-Systeme werden durch Firewalls geschützt, welche diese Server-Systeme gegen nicht betriebsnotwendige Zugriffe sichern. Diese Firewalls werden auf dedizierten und gehärteten, d.h. auf die betriebs-notwendigen Komponenten, Dienste und Schnittstellen beschränkten, Systemen betrieben und unverzüglich an neue technische Entwicklungen angepasst. Die Firewalls arbeiten mit einer regelbasierten Paketfilterung und stellen sicher, dass der zur Anwendung kommende Regel-satz die Kommunikation von und zu den informationsverarbeitenden Systemen des Auftragsverarbeiters mittels expliziter Freigaben ("White List") auf die minimal für den Betrieb dieser Systeme notwendigen Verbindungen eingeschränkt ist. Änderungen an der Konfiguration der Firewall und/oder dem zur Anwendung kommenden Regelsatz werden während der Laufzeit des Hauptvertrags dauerhaft und nachvollziehbar ("revisionssicher") dokumentiert.

6.3 Sämtliche gegebenenfalls vom Auftragsverarbeiter zur Durchführung dieser AV verwendete Software wird aktualisiert gehalten und sicherheitsrelevante Aktualisierungen (insbesondere Updates, Patches, Fixes) werden unverzüglich eingespielt, nachdem diese vom Hersteller der Software allgemein verfügbar gemacht und vom Auftragsverarbeiter im Rahmen eines dem Stand der Technik entsprechenden Verfahren getestet werden.

6.4 Originaldokumente, die VF-Daten enthalten, sowie beim Auftragsverarbeiter rechtmäßig auf informationsverarbeitenden Systemen gespeicherte VF-Daten werden durch technische und organisatorische Maßnahmen vor Verlust durch zufällige, fahrlässige oder vorsätzliche Löschung oder Veränderung geschützt.

6.5 Sicherungskopien von beim Auftragsverarbeiter rechtmäßig auf informationsverarbeitenden Systemen gespeicherten VF-Daten werden nach denselben Maßgaben wie Originaldaten behandelt, insbesondere gegen unbefugten Zugriff gesichert.

7 Order control

7.1 The persons employed by Processor in the execution of this DPA shall be trained comprehensively in regard to the general principles as well as the specific data protection requirements resulting from this DPA, including data safety, prior to being employed by Processor in the execution of this DPA and afterwards on a regular basis.

7.2 At the end of and based on the training process set out in clause 7.1, the persons employed by Pro-cessor in the execution of this DPA shall be obligated to confidentiality and protection of personal data. This obligation shall encompass secrecy of telecommunications and its associated principles and requirements regarding confidentiality of telecommunication if this is required subject to provisions concerning the specific order, especially if the order includes accessing traffic data, e.g. in form of itemised bills of Vodafone customers.

7.3 Execution of the trainings and obligations set out in clause 7.1 shall be documented in tamper-proof manner for the duration of the Master Agreement.

8 Encryption

If the VF Data has to be encrypted in accordance with this DPA, Processor utilises, subject to prior other agreements with Vodafone, a procedure that is recommended in the "Technical Guideline: Cryptographic Mechanisms: Recommendations and Key Lengths, BSI TR-02102" of the German Federal Office for Information Security (BSI) as amended and Processor shall at least comply with the following encryption standards:

- in symmetric block ciphers AES with a key length of 256 bit in the operating modes CBC or CFB;
-
- in asymmetric ciphers the procedure RSA with a key length of at least 2048 bit; and
- for hash procedures SHA-2.

9 Deletion

9.1 If Processor is, under this DPA, obliged to delete VF Data, Processor shall

(a) execute data protection regulation-compliant, irreversible deletion of any and all deletable electronic data carriers (especially hard drives, USB sticks, floppy discs, tapes) that contain VF Data;

(b) realise long-lasting and irreversible removal of VF Da-ta from database or file systems as well as from any and all other deletable storage media; an

(c) destroy any and all paper documents or other data carriers that contain VF Data and cannot be deleted under letter (a) or (b) of this clause 9.1 (including any misprints, memory cards, USB sticks, etc. that contain VF Data) using a commercially available file shredder compliant with security class 3 in accordance with DIN standard 66399 or an at least equivalent procedure.

9.2 Deletion shall be documented with undue delay after its execution, in particular the time of deletion and the deleted data shall be documented.

7 Auftragskontrolle

7.1 Über die allgemeinen Grundsätze sowie über die sich aus dieser AV ergebenden spezifischen Anforderungen des Datenschutzes, einschließlich der Datensicherheit, werden die beim Auftragsverarbeiter zur Durchführung dieser AV beschäftigten Personen vor dem Einsatz beim Auftragsverarbeiter zur Durchführung dieser AV und sodann regelmäßig umfassend geschult.

7.2 Am Ende und auf Grundlage des in Ziffer 7.1 festgelegten Schulungsprozesses werden die beim Auftragsverarbeiter zur Durchführung dieser AV beschäftigten Personen auf die Vertraulichkeit und den Schutz personenbezogener Daten verpflichtet. Diese Verpflichtung erstreckt sich auf das Fernmeldegeheimnis und die damit verbundenen Grundsätze und Anforderungen an die Vertraulichkeit der Telekommunikation, wenn dies nach Maßgabe des konkreten Auftrags erforderlich ist, insbesondere wenn der Auftrag den Zugriff auf Verkehrsdaten, z.B. in Form des Zugriffs auf Einzelverbin-dungsnachweise der Kunden von Vodafone, umfasst.

7.3 Die Durchführung der in Ziffer 7.1 festgelegten Schulungen und Verpflichtungen wird während der Laufzeit des Hauptvertrages revisionssicher dokumentiert.

8 Verschlüsselung

Besteht nach Maßgabe dieser AV eine Pflicht zur Verschlüsselung von VF-Daten, wendet der Auftragsverarbeiter, vorbehaltlich der vorherigen anderweitigen Ab-sprache mit Vodafone, einen Verfahren an, welches in der „Technischen Richtlinie: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, BSI TR-02102" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der jeweils aktuell gültigen Fassung empfohlen wird, und hält dabei zumindest folgende Verschlüsselungsstandards ein:

- bei symmetrischen Blockchiffren AES mit einer Schlüssellänge von 256 Bit in den Betriebsarten CBC oder CFB;
- bei asymmetrischen Chiffren das Verfahren RSA mit einer Schlüssellänge von mindestens 2048 Bit; und
- für Hash-Verfahren SHA-2.

9 Löschung

9.1 Besteht nach Maßgabe dieser AV für den Auftragsverarbeiter eine Pflicht zur Löschung von VF-Daten, wird der Auftragsverarbeiter

(a) die datenschutzgerechte nicht wieder herstellbare Löschung sämtlicher, VF-Daten enthaltender, löschbaren elektronischen Datenträger (insbesondere Festplatten, USB-Sticks, Disketten, Bänder) durchführen;

(b) die nachhaltige und irreversible Entfernung von VF-Daten aus Datenbank- oder File-Systemen sowie aus allen anderen löschbaren Speichermedien realisieren; und

(c) sämtliche, VF-Daten enthaltende Papierdokumente und sonstige nicht-gemäß Buchstabe (a) oder (b) dieser Ziffer 9.1 löschbaren Datenträger (einschließlich sämtlicher VF-Daten enthaltener Fehldrucke, Speicherkarten, USB-Sticks, etc.) mit einem handelsüblichen Dokumentenvernichter gemäß der Sicherheitsstufe 3 gemäß DIN 66399 oder einem mindestens gleichwertigen Verfahren vernichten.

9.2 Die Löschung wird unverzüglich nach ihrer Durchführung dokumentiert, insbesondere unter Angabe des Lösch-zeitpunkts und der gelöschten Daten.

10 Documentation and record proofs

All documents and records that are to be prepared subject to this toMs-document shall be made available to Vodafone immediately on request, unless regulated otherwise in this toMs-document.

10 Dokumentations- und Protokollierungsnachweise

Nach dem vorliegenden toMs-Dokument zu erstellende Dokumentationen und Protokolle werden Vodafone auf Anfrage unverzüglich zur Verfügung gestellt, sofern sich nicht aus dem vorliegenden toMs-Dokument etwas Abweichendes ergibt.

11 Special obligations for call centres

Insofar as Processor provides call centre services, they shall also implement the following technical and organisational measures.

11 Besondere Verpflichtungen für Callcenter

Sofern der Auftragsverarbeiter Callcenter-Dienstleistungen erbringt, hat er zusätzlich die folgenden technischen und organisatorischen Maßnahmen umzusetzen.

11.1 Access to the premises of Processor that are used for execution of this DPA shall be limited to the persons required for execution of the DPA.

11.1 Der Zutritt zu den Räumlichkeiten des Auftragsverarbeiters, die zur Durchführung dieser AV verwendet werden, ist auf die zur Durchführung der AV erforderlichen Personen beschränkt.

11.2 Original documents that contain VF Data shall be issued to the persons providing the services by the supervising personnel responsible for the process and shall be collected again by these after completion of work.

11.2 Originaldokumente, die VF-Daten enthalten, werden durch die den Prozess verantwortlich leitenden Personen an die zur Leistungserbringung eingesetzten Personen herausgegeben und von diesen nach Arbeitsschluss wieder entgegengenommen.

11.3 The client systems of the persons employed by Processor in the execution of this DPA shall be designed so that access to the Internet is limited to the extent required for performance of the service. In particular, accessing third-party services offered online, especially translation services, storage services or web mailer, are disabled by technical means.

11.3 Die Client-Systeme der für den Auftragsverarbeiter bei der Durchführung dieser AV beschäftigten Personen ist so gestaltet, dass der Zugang zum Internet auf das zur Leistungserbringung erforderliche Maß beschränkt ist Insbesondere ist der Zugang zu über das Internet angebotenen Diensten Dritter, insbesondere Übersetzungs-dienste, Speicherdienste oder Web Mailer technisch unterbunden.

11.4 The applications made available to the persons employed by Processor in the execution of this DPA on the client systems shall be limited to the necessary extent. Besides any software used by Processor to provide the service in coordination with Vodafone, there is no application available that can be used to import VF Data from Vodafone systems and to disclose them without authorisation (e.g. snipping tool).

11.4 Die den bei der Durchführung dieser AV beim Auftragsverarbeiter beschäftigten Personen auf den Client-Systemen bereitgestellten Applikationen sind auf das erforderliche Maß beschränkt. Es ist, neben der ggf. vom Auftragsverarbeiter in Absprache mit Vodafone zur Leistungserbringung eingesetzten Software, keine Applikation verfügbar, über welche, VF-Daten aus den Systemen von Vodafone übernommen und unbefugt weitergeben werden können (z.B. Snipping Tool).

11.5 On clients used by Vodafone to execute this DPA, technical measures such as the use of a software for interface control or complete deactivation of interfaces (especially USB ports, card readers, PCMCIA, IEEE1394, Bluetooth and WLAN) are used on principle to make it impossible to transfer VF Data to external media. Where the use of such interfaces and storage media is required in individual cases and after consultation with Vodafone, VF Data shall only be transferred to and stored on these media for the purpose agreed with Vodafone on a case-by-case basis and only in encrypted form subject to clause 8.

11.5 Auf den vom Auftraggeber zur Durchführung dieser AV eingesetzten Clients ist durch technische Maßnahmen, wie beispielsweise den Einsatz einer Software zur Schnittstellenkontrolle oder eine vollständige Deaktivierung der Schnittstellen (insbesondere USB-Ports, Card Reader, PCMCIA, IEEE1394, Bluetooth sowie WLAN) die Übertragung von VF-Daten auf externe Medien technisch grundsätzlich unterbunden. Soweit die Nutzung solcher Schnittstellen und Speichermedien im Einzelfall und nach Absprache mit Vodafone erforderlich ist, werden VF-Daten lediglich zu den im Einzelfall mit Vodafone abgestimmten Zweck lediglich in gem. Ziffer 8 verschlüsselter Form auf diese Medien und dort gespeichert.

11.6 On the premises of Processor that are used for execution of this DPA, access to technical equipment which can be used to duplicate (especially photocopiers) as well as printers is only granted subject to a restrictive and technically implemented access concept, e.g. by access code, and access to these devices is organised in such a manner as to be restricted to specially instructed employees (e.g. project or team leaders, management) and to the fulfilment of their tasks.

11.6 In den zur Durchführung dieser AV verwendeten Räumlichkeiten des Auftragsverarbeiters ist der Zugang zu technischen Einrichtungen, die zur Anfertigung von Kopien geeignet sind (insbesondere Fotokopierer) sowie zu Druckern lediglich nach Maßgabe eines restriktiven und technisch implementierten Zugangskonzepts, z.B. mit einem Zugangscode, und so realisiert, dass der Zugang zu diesen Geräten auf besonders instruierte Mitarbeiter (z.B. Projekt- oder Teamleiter, Führungskräfte) und auf die Er-füllung von deren Aufgaben beschränkt ist.