ALLEGATO B

Disciplinare tecnico in materia di misure minime di sicurezza (Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

ANHANG B

Technische Vorschriften im Bereich der Mindestsicherheitsmaßnahmen (Art. 33 bis 36 des Datenschutzkodex)

Datenverarbeitung mit elektronischen Mitteln

Spezifische Verfahren, die vom Rechtsinhaber, vom eventuell namhaft gemachten Verantwortlichen und vom Beauftragten bei der Datenverarbeitung mit elektronischen Mitteln angewandt werden müssen:

Authentifizierungssysteme

1. Die Verarbeitung personenbezogener Daten mit elektronischen Mitteln ist jenen Beauftragten erlaubt, die über Mittel zur Authentifizierung verfügen, mit denen sie Authentifizierungsverfahren in Bezug auf eine bestimmte oder mehrere zusammenhängende Verarbeitungen durchführen können.

2. Die Mittel zur Authentifizierung bestehen aus einem Code zur Identifizierung des Beauftragten, verbunden mit einem nur diesem bekannten Kennwort, aus einer Authentifizierungsvorrichtung, die sich im Besitze des Beauftragten befindet und nur von diesem verwendet werden darf, eventuell verbunden mit einem Identifizierungscode oder einem Kennwort, oder schließlich aus einem biometrischen Merkmal des Beauftragten, eventuell verbunden mit einem Identifizierungscode oder einem Kennwort.

3. Jedem Beauftragten werden ein oder mehrere Mittel zur Authentifizierung zugewiesen oder sie werden auf ihn persönlich bezogen.

4. In den schriftlichen Anweisungen für die Beauftragten muss festgehalten werden, dass sie die notwendigen Vorkehrungen zu treffen haben, um die Geheimhaltung des persönlichen Bestandteiles des Mittels zur Authentifizierung und die gewissenhafte Verwahrung der Vorrichtungen, in deren Besitz sie sind und die nur sie verwenden dürfen, zu gewährleisten.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

5. Ist vom Authentifizierungssystem ein Kennwort vorgesehen, so muss es aus mindestens acht Zeichen oder, falls das elektronische Mittel dies nicht zulässt, aus der maximal erlaubten Anzahl an Zeichen bestehen. Es darf keine Informationen enthalten, die leicht Rückschlüsse auf den Beauftragten zulassen, und muss von diesem bei der ersten Anwendung und anschließend wenigstens alle sechs Monate geändert werden. Bei der Verarbeitung von sensiblen und von Gerichtsdaten muss das Kennwort alle drei Monate geändert werden.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

6. Der eventuell verwendete Identifizierungscode darf nicht anderen Beauftragten zugewiesen werden, auch nicht zu verschiedenen Zeiten.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

7. Werden Mittel zur Authentifizierung mindestens sechs Monate lang nicht mehr verwendet, müssen sie deaktiviert werden, sofern es sich nicht um solche handelt, die von Anfang an nur zum Zwecke der technischen Verwaltung genehmigt wurden.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

8. Die Mittel zur Authentifizierung sind auch dann zu deaktivieren, wenn der Beauftragte die Eigenschaft verliert, auf Grund welcher er Zugang zu den personenbezogenen Daten hatte.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

9. Den Beauftragten sind Anweisungen zu geben, um zu vermeiden, dass das elektronische Mittel während eines Verarbeitungsvorganges unbewacht und für andere zugänglich ist.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'in-

10. Ist der Zugang zu den Daten und zu den elektronischen Mitteln nur über einen persönlichen Bestandteil des Mittels zur Authentifizierung möglich, so sind vorher angemessene schriftliche Anweisungen zu geben, um einwandfrei die Modalitäten festzulegen, mit denen der Rechtsinhaber die Verfügbarkeit der Daten oder elektronischen Mittel gewährleisten kann, wenn bei längerer Abwesenheit oder Verhinderung des Beauftragten ein Zugriff aus Gründen der Operativität und der Systemsicherheit unbedingt dringend erforderlich ist. In diesem Fall müssen die Kopien der Authentifizierungsmittel so verwahrt werden, dass ihre Geheimhaltung gewährleistet ist. Die mit der Verwahrung betrauten Personen sind rechtzeitig schriftlich zu

tervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

bestellen und müssen den Beauftragten umgehend über jeden Eingriff informieren.

11. Die unter den vorhergehenden Punkten angeführten Bestimmungen über das Authentifizierungssystem und jene über das Bewilligungssystem sind nicht auf die Verarbeitung von personenbezogenen Daten anzuwenden, die für die Verbreitung bestimmt sind.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Bewilligungssystem

12. Wurden für die Beauftragten verschiedene persönliche Benutzungsberechtigungen festgelegt, so ist ein Bewilligungssystem anzuwenden.

13. Die persönlichen Benutzungsberechtigungen sind für jeden Beauftragten oder für homogene Gruppen von Beauftragten vor Verarbeitungsbeginn auszumachen und zu konfigurieren, sodass der Zugriff auf jene Daten beschränkt ist, die für die Verarbeitungsvorgänge gebraucht werden.

14. Regelmäßig, mindestens aber jährlich, ist zu überprüfen, ob die Voraussetzungen für die Beibehaltung der persönlichen Benutzungsberechtigungen noch gegeben sind.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità

Andere Sicherheitsmaßnahmen

15. Bei der periodischen, mindestens jährlichen Aktualisierung der Festlegung des Verarbeitungsbereichs für die einzelnen Beauftragten und für die mit der Verwaltung oder Instandhaltung der elektronischen Mittel betrauten Personen kann die Liste der Beauftragten auch nach homogenen Aufgabenbereichen und entsprechenden persönlichen Benutzungsberechtigungen erstellt werden.

16. Die personenbezogenen Daten sind gegen jedes Eindringen und gegen die Wirkung von Programmen laut Artikel 615-quinquies des Strafgesetzbuches durch den Einsatz geeigneter elektronischer Mittel zu schützen, die mindestens halbjährlich auf den neuesten Stand gebracht werden müssen.

17. Die periodische Aktualisierung der Computerprogramme zur Vorbeugung der Störungsan-

di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

fälligkeit der elektronischen Mittel und zur Behebung von Fehlern hat mindestens jährlich zu erfolgen. Bei der Verarbeitung von sensiblen und von Gerichtsdaten muss die Aktualisierung mindestens halbjährlich erfolgen.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

18. Es sind organisatorische und technische Anweisungen zu geben, nach denen die Datensicherung mindestens wöchentlich durchgeführt werden muss.

Documento programmatico sulla sicurezza

Sicherheitsplan

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19. Bis 31. März jeden Jahres haben Rechtsinhaber, die sensible oder Gerichtsdaten verarbeiten, auch durch den eventuell namhaft gemachten Verantwortlichen, einen Sicherheitsplan zu erstellen, in dem angemessene Informationen enthalten sind über

19.1. l'elenco dei trattamenti di dati personali;

19.1. das Verzeichnis der Verarbeitungen von personenbezogenen Daten;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.2. die Verteilung der Aufgaben und der Verantwortung im Bereich der Einrichtungen, die mit der Datenverarbeitung betraut sind;

19.3. l'analisi dei rischi che incombono sui dati;

19.3. die Abschätzung der Risiken, denen die Daten ausgesetzt sind;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.4. die Maßnahmen, die zu treffen sind, um die Unversehrtheit und die Verfügbarkeit der Daten sowie die Sicherheit der Bereiche und Räume, die für die Verwahrung und Zugänglichkeit dieser Daten relevant sind, zu gewährleisten;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.5. die Kriterien und Vorgangsweisen zur Wiederherstellung der Daten, wenn diese vernichtet oder gemäß Punkt 23 beschädigt wurden;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.6. die Planung von Ausbildungsmaßnahmen für die mit der Verarbeitung Beauftragten, um sie über folgendes aufzuklären: die Risiken, denen die Daten ausgesetzt sind, die verfügbaren Mittel zur Verhinderung von Schadensfällen, die grundlegenden Datenschutzbestimmungen in Bezug auf die jeweilige Tätigkeit, die daraus folgende Verantwortung für den Einzelnen und die Möglichkeiten, sich laufend über die vom Rechtsinhaber angewandten Mindestsicherheitsmaßnahmen zu informieren. Die Ausbildung ist bereits bei Dienstantritt zu planen sowie bei jedem Aufgabenwechsel und bei der Einführung neuer für die Verarbeitung personenbezo-

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

gener Daten relevanter Mittel;

19.7. die Kriterien, die zu befolgen sind, um die Anwendung der Mindestsicherheitsmaßnahmen auch dann zu gewährleisten, wenn Verarbeitungen von personenbezogenen Daten unter Befolgung des Datenschutzkodex außerhalb der Einrichtungen des Rechtsinhabers durchgeführt werden;

19.8. wenn es sich um personenbezogene Daten laut Punkt 24, die Aufschluss über den Gesundheitszustand oder das Sexualleben geben können, handelt, die Kriterien zur Chiffrierung oder zur Trennung dieser Daten von den anderen auf die betroffene Person bezogenen Daten.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei da-

Weitere Maßnahmen bei der Verarbeitung von sensiblen oder von Gerichtsdaten

20. Die sensiblen oder Gerichtsdaten sind durch den Einsatz geeigneter elektronischer Mittel gegen unbefugten Zugang laut Artikel 615-ter des Strafgesetzbuches zu schützen.

21. Es sind organisatorische und technische Anweisungen für die Verwahrung und die Benutzung der beweglichen Datenträger, auf denen die Daten gespeichert sind, zu geben, um einen unbefugten Zugriff oder unerlaubte Verarbeitungen zu verhindern.

22. Bewegliche Datenträger, die sensible oder Gerichtsdaten enthalten und nicht gebraucht werden, sind zu vernichten oder unbrauchbar zu machen oder sie dürfen von anderen Beauftragten, die nicht zur Verarbeitung dieser Daten befugt sind, wieder verwendet werden, wenn alle vorher darauf enthaltenen Informationen nicht mehr lesbar und technisch auf keine Weise wieder herstellbar sind.

23. Es sind geeignete Maßnahmen zu treffen, um innerhalb bestimmter Zeiträume, die mit den Rechten der betroffenen Personen vereinbar sind, spätestens aber innerhalb von sieben Tagen, einen erneuten Zugriff auf die Daten zu gewährleisten, wenn diese oder die elektronischen Mittel beschädigt sind.

24. Die Gesundheitseinrichtungen und die Personen, die einen Gesundheitsberuf ausüben, ver-

ti idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

arbeiten die in Verzeichnissen, Registern oder Datenbanken enthaltenen Daten, die Aufschluss über den Gesundheitszustand und das Sexualleben geben können, nach Artikel 22 Absatz 6 des Datenschutzkodex, auch um zu ermöglichen, dass diese Daten getrennt von den anderen personenbezogenen Daten verarbeitet werden, die die direkte Identifizierung der betroffenen Personen ermöglichen. Die Daten über die genetische Identität dürfen ausschließlich in geschützten Räumen verarbeitet werden, zu denen nur die mit der Verarbeitung Beauftragten und die ausdrücklich dazu ermächtigten Personen Zutritt haben; diese Daten dürfen außerhalb der für die Verarbeitung vorbehaltenen Räume nur in Behältern mit Schließ- oder gleichwertigen Vorrichtungen befördert werden; bei elektronischer Übermittlung müssen diese Daten chiffriert werden.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Schutz- und Garantiemaßnahmen

25. Nimmt ein Rechtsinhaber zur Anwendung von Mindestsicherheitsmaßnahmen die Mitarbeit von Personen in Anspruch, die nicht zur eigenen Einrichtung gehören, so muss er von der installierenden Person eine Beschreibung des erfolgten Eingriffes erhalten, aus der hervorgeht, dass die Bestimmungen dieser technischen Vorschriften eingehalten wurden.

26. Der Rechtsinhaber hat im eventuell vorgeschriebenen Begleitbericht zum Jahresabschluss festzuhalten, dass der Sicherheitsplan erstellt oder aktualisiert wurde.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno

Verarbeitung ohne elektronische Mittel

Spezifische Verfahren, die vom Rechtsinhaber, vom eventuell namhaft gemachten Verantwortlichen und vom Beauftragten bei der Datenverarbeitung ohne elektronische Mittel angewandt werden müssen:

27. Den Beauftragten sind schriftliche Anweisungen zu geben, um die Überwachung und die Verwahrung der Akte und Dokumente, die personenbezogene Daten enthalten, während der gesamten für die Verarbeitungsvorgänge erforderlichen Zeit zu gewährleisten. Bei der periodi-

annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

schen, mindestens jährlichen Aktualisierung der Festlegung des Verarbeitungsbereichs für die einzelnen Beauftragten kann die Liste der Beauftragten auch nach homogenen Aufgabenbereichen und entsprechenden persönlichen Benutzungsberechtigungen erstellt werden.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

28. Werden Akte und Dokumente, die personenbezogene sensible oder Gerichtsdaten enthalten, den mit der Verarbeitung Beauftragten zur Ausführung ihrer Aufgaben anvertraut, müssen sie von diesen bis zur Rückgabe in der Weise überwacht und aufbewahrt werden, dass andere, nicht dazu befugte Personen keinen Zugriff darauf haben. Nach Abschluss des jeweiligen Verarbeitungsvorganges sind sie zurückzugeben.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

29. Der Zugang zu Archiven, in denen sensible oder Gerichtsdaten enthalten sind, muss kontrolliert werden. Personen, die mit jeglichem Rechtstitel nach der Öffnungszeit zugelassen werden, müssen identifiziert und registriert werden. Werden die Archive nicht mit elektronischen Mitteln zur Kontrolle der Zugänge oder durch Aufsichtspersonen überwacht, müssen die Personen, die auf das Archiv zugreifen, vorher dazu ermächtigt werden.