Kriterienkatalog CH-Version

(Schweiz; Stand Januar 2018)

Das Datenschutzgütesiegel „ePrivacyseal – geprüfter Datenschutz CH“ der ePrivacyseal GmbH zertifiziert dem Lizenzberechtigten, dass das Produkt und System, die geprüft wurden, mit den im nachfolgenden Kriterienkatalog näher spezifizierten Kriterien, die sich an den Anforderungen des Schweizer Datenschutzrechtes orientieren, im Einklang stehen. Im Einzelnen wird damit die Einhaltung folgender Bestimmungen bestätigt:

I. Allgemeine Grundsätze

1. Verhältnismäßigkeit

Der Lizenzberechtigte darf nur diejenigen Daten bearbeiten, die für die Erfüllung der Aufgabe bzw. die Erreichung des Zwecks unbedingt notwendig und dafür geeignet sind (Datensparsamkeit, Datenvermeidung, Art. 4 Abs. 2 DSG). Bei der Auswahl und Gestaltung des Systems ist daher der Grundsatz, nur so wenig Personendaten wie möglich zu erheben, zu verarbeiten, zu nutzen und zu berücksichtigen.

- Erfolgt die Bearbeitung von Personendaten in den Fällen, in denen die Identität der Person für den verfolgten Zweck nicht benötigt wird, in pseudonymisierter oder anonymisierter Form?
- Ist vorab geprüft worden, ob nicht auch die Möglichkeit der Anonymisierung bzw. Pseudonymisierung dieser Personendaten in Betracht kommt?
- Werden nur die Personendaten erhoben bzw. verarbeitet und genutzt, die für den Verwendungszweck unbedingt erforderlich sind?
- Sind ausreichende Maßnahmen getroffen worden, die Menge der zu verarbeitenden Daten möglichst gering zu halten? Wenn ja, welche?
- Werden bei jedem Verwendungsschritt ggf. nicht mehr für den ursprünglichen Verarbeitungszweck erforderliche Daten umgehend gelöscht?
- Wie wird die Löschung bzw. Anonymisierung und Pseudonymisierung der Daten umgesetzt?
- Erfolgt die Anonymisierung bzw. Pseudonymisierung zum frühestmöglichen Zeitpunkt?
- Ist im Falle einer Pseudonymisierung von Daten gewährleistet, dass diese Daten nicht mit wenig Aufwand wieder „depseudonymisiert“ werden können?
- Sind die Mitarbeiter hinsichtlich der Grundsätze der Datenvermeidung und Datensparsamkeit ausreichend geschult?
- Werden nicht benötigte Personendaten vernichtet oder anonymisiert, soweit keine Archivierungs- oder Aufbewahrungspflichten bestehen?

2. Transparenz

Das Bearbeiten von Personendaten soll rechtmässig und transparent erfolgen. Das heißt, in keinem Fall ohne Kenntnis der betroffenen Person oder für andere als bei der Beschaffung angegebene Zwecke.

a) Beschreibung des Produkts / der Dienstleistung

Dem Nutzer muss eine klar verständliche Beschreibung des angebotenen Produkts bzw. der angebotenen Dienstleistung zur Verfügung gestellt werden.

- Wird dem Nutzer eine klar verständliche Beschreibung des angebotenen Produkts bzw. der angebotenen Dienstleistung zur Verfügung gestellt?
- Wird diese Beschreibung immer auf dem aktuellen Stand gehalten?
- Wird in dieser Beschreibung der Fluss der Datenbearbeitung sowie etwaige Datenübermittlungen bzw. Zugriffsrechte hinreichend deutlich?

b) Informationspflichten

Der Lizenzberechtigte muss die folgenden Informationspflichten erfüllen, soweit Gegenstand der Zertifizierung ein Online-Angebot ist:

- Enthält das Online-Angebot eine ausreichende Anbieterkennzeichnung (Firma, Sitz, Adresse des Dienstleistungserbringers)?
- Sind Angaben vorhanden, die eine rasche Kommunikation mit dem Anbieter ermöglicht (Telefonnummer, e-Mail-Adresse, verantwortliche Stelle oder Person)?
- Wird kommerzielle Kommunikation (also Werbung, z.B. per E-Mail) klar als solche gekennzeichnet und ist das Unternehmen, welches diese verschickt, klar identifizierbar?
- Soweit Angebote zur Verkaufsförderung wie Preisnachlässe, Zugaben und Geschenke angeboten werden: Sind diese für den Nutzer klar erkennbar sowie sind die Bedingungen für ihre Inanspruchnahme leicht zugänglich, klar und eindeutig?

- Ist sichergestellt, dass Preisausschreiben und Gewinnspiele nicht gegen das Lotteriegesetz verstossen?
- Wird in Werbe-E-Mails weder der Absender, noch der kommerzielle Charakter der Nachricht verschleiert?
- Wird der Nutzer über die Möglichkeit aufgeklärt, die Verwendung seiner Adresse (Postanschrift/E-Mail Adresse) zu Werbezwecken zu untersagen?
- Wird der Nutzer in klar verständlichen Worten im Rahmen einer Datenschutzerklärung über die Art und den Umfang der Beschaffung der Personendaten und insbesondere den Zweck ihrer Bearbeitung hinreichend aufgeklärt?
- Erfolgt die Information des Nutzers und die Bearbeitung von Personendaten nach Treu und Glauben, das heißt, ohne Zwang und ohne irreführende Elemente?
- Ist insbesondere die Unterrichtung über die Datenbeschaffung korrekt und vollständig?
- Falls die Daten auch außerhalb der Schweiz verarbeitet werden: Wird der Nutzer darüber informiert?
- Falls sich die Server des Anbieters eines Auswertungstools im Ausland befinden: Werden die datenschutzrechtlichen Regelungen zum grenzüberschreitenden Datentransfer beachtet (Art. 6 DSG)?
- Falls Nutzungsprofile erstellt werden:
    - Wird der Nutzer im Rahmen einer jederzeit abrufbaren Datenschutzerklärung auf die Verwendung eines Auswertungs- und Tracking-Tools sowie Art und Umfang der gesammelten Daten und sein Widerspruchsrecht hingewiesen?
    - Nimmt der Webseiten-Betreiber durch entsprechende Einstellungen im Programmcode die Kürzung der IP-Adressen vor oder lässt er diese vornehmen?

- Erfolgt eine ausreichende Information über Cookies, Weblogs, Analyse- bzw. Tracking-Dienste, etc.?

- Ist die Datenschutzerklärung jederzeit abrufbar?
- Sofern eine solche Analyse durch einen Dritten erfolgt:
- Wird der Nutzer über die Bearbeitung der Personendaten durch einen Dritten informiert?
- Ist eine Vereinbarung mit dem Drittanbieter vorhanden, die regelt, dass der Drittanbieter des Tools die Daten nur so bearbeitet, wie es der Betreiber der Webseite selbst tun dürfte?
- Ist sichergestellt, dass keine gesetzlichen oder vertraglichen Geheimhaltungspflichten zwischen Betreiber der Website und dem Nutzer bestehen, die eine Datenbearbeitung durch einen Dritten verbieten würden? Wurden solche Pflichten durch eine Einwilligung des Nutzers / eine Entbindung des Anbieters von der Geheimhaltung aufgehoben?
- Soweit eine Weitervermittlung der Personendaten zu einem anderen Dienstleister erfolgt:
    - Wird dem Nutzer diese Weitervermittlung (bspw. in der Datenschutzerklärung) angezeigt?
    - Geschieht dies in verständlicher Weise?

3. Zweckbindung und Zweckänderung

Der Lizenzberechtigte hat bei der Datenbearbeitung (insbesondere der Datenspeicherung, -verarbeitung und -nutzung) sicherzustellen, dass die erhobenen Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde, gesetzlich vorgesehen ist oder aus den Umständen ersichtlich ist.

- Hat der Inhaber der Datensammlung den Zweck der Datensammlung und die Mittel und Methoden der Bearbeitung definiert und ist dies entsprechend dokumentiert (bspw. Umgang mit Datenbeschaffung und -bearbeitung als Teil der Geschäftspolitik, Beschluss der Geschäftsführung)?
- Ist für die betroffene Person der Zweck der Datenbeschaffung bzw. ob und wann Daten, die sie betreffen, beschafft werden, erkennbar? Liegt bspw. eine Datenschutzerklärung vor, welche auf der Website leicht zugänglich platziert ist?

- Ist sichergestellt, dass die erhobenen Daten nur gemäß ihrer Zweckbestimmung bearbeitet werden?
- Wird die Bearbeitung der Daten protokolliert, um ggf. Zweckänderungen nachweisen zu können?
- Werden nachträgliche Änderungen des ursprünglichen Zwecks, die entsprechenden Informationshandlungen und neue Einwilligungen dokumentiert?

4. Trennungsgebot

Der Lizenzberechtigte hat zu gewährleisten, dass bei seiner Datenbearbeitung das Trennungsgebot beachtet wird. Das Trennungsgebot verlangt, dass die Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt voneinander bearbeitet werden können.

- Falls Personendaten unterschiedlichen Ursprungs an einer zentralen Stelle gespeichert werden: Ist technisch bzw. organisatorisch gewährleistet, dass die Selektion einzelner Datensätze nur und ausschließlich zweckgebunden erfolgen kann?
- Sofern es sich um IT-Dienstleister handelt: Ist bei mehreren Kunden gewährleistet, dass die Datenverarbeitungssysteme so ausgestaltet sind, dass sich die Datenbereiche der Kunden nicht versehentlich überschneiden und dadurch Daten des einen Kunden von anderen mitausgelesen werden können?

II. Rechtmäßigkeit der Bearbeitung von Personendaten

1. Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung von Personendaten (Datenbearbeitung)

a) Personendaten werden nur bearbeitet, wenn ein Rechtfertigungsgrund vorliegt, das heißt, wenn die Einwilligung der betroffenen Person, ein überwiegendes privates oder öffentliches Interesse oder eine gesetzliche Grundlage vorliegt.

b) Sofern eine Einwilligung des Betroffenen einzuholen ist, ist sicherzustellen, dass die Einwilligung nach angemessener Information freiwillig erfolgt. Bei der Einholung der Einwilligung ist sicherzustellen, dass zugleich auf den vorgesehenen Zweck der Datenbearbeitung sowie, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hingewiesen wird. Der Lizenzberechtigte muss ferner sicherstellen, dass die Einwilligung in der gesetzlich vorgesehenen Form eingeholt wird.

- Liegt ein überwiegendes privates oder öffentliches Interesse oder eine gesetzliche Grundlage als Rechtfertigungsgrund für die Datenbearbeitung vor?
- Falls dies nicht der Fall ist: Ist eine gültige Einwilligung der betroffenen Person eingeholt worden?
- Ist die Formulierung einer vorgegebenen Einwilligungserklärung hinreichend konkret, d. h. sind die erforderlichen Angaben zu der datenverarbeitenden Stelle, der Art von Daten, die bearbeitet werden sollen, zur geplanten Übermittlung sowie zu den Empfängern dieser etwaigen Übermittlung, Zweck der Datenbearbeitung sowie zudem auch ein Hinweis auf die Widerrufbarkeit dieser Einwilligung sowie deren Freiwilligkeit vorhanden?
- Ist die Einwilligung bei besonders schützenswerten Personendaten oder Persönlichkeitsprofilen „ausdrücklich“ erteilt worden (Art. 4 Abs. 5 DSG)?

c) Für die Einwilligung zur Bearbeitung von gewöhnlichen Personendaten besteht keine Formvorschrift, allerdings sollte die Einwilligung aus Beweisgründen nachweisbar sein (schriftliche Einwilligung; E-Mail; Klick).

- Sofern diese Einwilligung zusammen mit anderen Erklärungen somit schriftlich bzw. elektronisch erteilt wird: Ist diese Einwilligung besonders hervorgehoben?
- Werden die Einwilligungen so gesammelt/archiviert, dass für jeden einzelnen Kunden bei Anfrage die gegebene Einwilligung als Nachweis-Beleg geliefert werden kann?

2. Besondere Arten von Personendaten

Sollte der jeweilige Lizenzberechtigte besonders schützenswerte Daten im Sinne von Art. 3 lit. c DSG oder Persönlichkeitsprofile im Sinne von Art. 3 lit. d DSG für eigene Geschäftszwecke bearbeiten oder nutzen, ist insbesondere sicherzustellen, dass zusätzlich zu den allgemeinen Grundsätzen gemäß Art. 4 ff und insbesondere Art. 13 DSG die Voraussetzungen der Art. 4 Abs. 5, 11a Abs. 3 lit.a, Art. 12 Abs. 2 lit.c und Art. 14 DSG eingehalten werden.

Besonders schützenswerte Personendaten gemäß Art. 3 lit. c DSG sind Daten über (1) die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, (2) die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, (3) Maßnahmen der sozialen Hilfe, (4) administrative oder strafrechtliche Verfolgungen und Sanktionen. Sofern diese verarbeitet werden sollen, hat die Einwilligung ausdrücklich zu erfolgen.

3. Rechtfertigungsgründe

Die Bearbeitung von Personendaten für eigene Geschäftszwecke ist, sofern der Betroffene nicht wirksam eingewilligt hat, zulässig, wenn:

- das Gesetz die Datenbearbeitung von Personendaten zulässt (gesetzlicher Rechtfertigungsgrund); ein überwiegendes privates oder öffentliches Interesse besteht (Art. 13 Abs. 1 DSG), bspw.:
    - in den in Art. 13 Abs. 2 DSG aufgeführten Fällen; sofern die Daten bearbeitende Person
        - in unmittelbarem Zusammenhang mit dem Abschluss oder der
        - Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet;

- mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben;

  - zur Prüfung der Kreditwürdigkeit einer anderen Person weder besonders schützenswerte Personendaten noch Persönlichkeitsprofile bearbeitet und Dritten nur Daten bekannt gibt, die sie für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen;
  - beruflich Personendaten ausschließlich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet;
  - Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet und die Ergebnisse so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind;

- wenn Daten über eine Person des öffentlichen Lebens gesammelt werden, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.

oder

- sofern Interessen von allgemein anerkanntem Wert vorliegen, z.B.
  - die Datenbearbeitung zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außer Stande ist, seine Einwilligung zu geben,
  - es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
  - die Datenbearbeitung zu Geltendmachung, Ausübung oder
  - Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des

Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder

- dies zur Durchführung wissenschaftlicher Forschungen erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht übernommen und unverhältnismäßigem Aufwand erreicht werden kann.
- Das Erheben von besonderen Arten personenbezogener Daten ist zudem zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen.

4. Erhebung und Verarbeitung von Nutzungsdaten sowie Erstellung von Nutzungsprofilen

Ruft ein Nutzer eine Website auf, werden Nutzungsdaten (Randdaten) generiert.

Es ist zu unterscheiden, zwischen Nutzungsdaten, die personenbezogen sind (Personendaten) und anonymisierten Nutzungsdaten. Die IP Adresse fällt unter den Begriff der Personendaten. Alle Nutzungsdaten, die mit der IP-Adresse verbunden werden können, gelten als Personendaten. Bei anonymisierten Daten kann der Bezug zu Personen nicht mehr hergestellt werden. Anonymisierte Daten gelten daher nicht als Personendaten. Diese können frei bearbeitet werden. Für die Bearbeitung von Personendaten, die bloß pseudonymisiert sind, ist eine Einwilligung notwendig.

Bei der Erhebung und Verarbeitung von personenbezogenen Nutzungsdaten ist sicherzustellen, dass die gelieferten Daten ausschliesslich zu den Auswertungszwecken des Webseiten-Betreibers genutzt werden (nicht für Zwecke von Dritten) und die Datensicherheit gewährleistet ist. Zudem muss der Betreiber der Webseite aufgrund des Erkennbarkeitsprinzips die Nutzer im Rahmen einer Datenschutzerklärung auf die Verwendung eines solchen Auswertungs-Tools sowie Art und Umfang der gesammelten

Daten hinweisen. Befinden sich die Server des Lizenzberechtigten des Auswertungstools im Ausland, sind darüber hinaus die datenschutzrechtlichen Regelungen zum grenzüberschreitenden Datentransfer zu beachten.

- Welche Nutzungsdaten werden erhoben?
- Durch wen werden diese Nutzungsdaten erhoben
- Werden diese Nutzungsdaten auch gespeichert? Wenn ja: Durch wen und für wie lange? Werden Nutzungsdaten im Ausland gespeichert?
- Wann werden die Nutzungsdaten gelöscht?
- Werden nur Nutzungsdaten erhoben, die für die Erbringung bzw. Abrechnung des angebotenen Dienstes erforderlich sind?
- Ist sichergestellt, dass die Nutzungsdaten zu keinem anderen Zweck als dem Nutzer bekannt gegebenen Zweck bearbeitet werden?
- Ist die Datenschutzerklärung in Bezug auf den Einsatz von Analyse- oder Tracking- Tools und die Auswertung der Personendaten vollständig und verständlich?
- Bei personenbezogenen Nutzungsdaten: Liegt die Einwilligung der betroffenen Person vor?
- Wird der Nutzer auf die Widerspruchsmöglichkeiten gegen die Erfassung durch das Analyse- oder Tracking-Tool hingewiesen?
- Nimmt der Webseiten-Betreiber durch entsprechende Einstellungen im Programmcode die Kürzung der IP-Adressen vor?
- Werden nur Nutzungsdaten gespeichert, die für die Abrechnung des angebotenen Dienstes erforderlich sind?
- Werden darüber hinaus auch Bestandsdaten erhoben?
- Sofern auch die IP-Adresse erhoben wird: von wem wird die IP-Adresse erhoben und zu welchem Zweck?
- Wird die IP-Adresse auch gespeichert? Wenn ja: für wie lange?
- Sofern Cookies eingesetzt werden:
    - Welche Arten von Cookies werden eingesetzt?
    - Kann der Nutzer dem Setzen der Cookies widersprechen?

    - Werden die in den Cookies gespeicherten Daten ausgelesen? Wenn ja: Erfolgt eine Speicherung dieser Daten? Zu welchem Zweck?
    - Muss der Nutzer Cookies aktivieren (Opt-in)? oder kann der Nutzer die Cookies zumindest wegbedingen resp. inaktivieren (Opt-out)?
- Sofern Analyse- bzw. Tracking-Dienste eingesetzt werden: Sind diese datenschutzrechtlich unbedenklich?

III. Gewährleistung der Betroffenenrechte

Der Nutzungsberechtigte hat zu gewährleisten, dass die gesetzlich verankerten Betroffenenrechte in effektiver Weise durchsetzbar sind und dass die dazu erforderlichen technischen und organisatorischen Maßnahmen eingerichtet worden sind. Dazu zählen insbesondere die folgenden Rechte bzw. Verpflichtungen:

1. Recht auf Auskunft

- Sind alle Informationen, die der Nutzer benötigt, um seinen Auskunftsanspruch geltend zu machen, leicht auffindbar?
- Bezieht sich die Auskunftsmöglichkeit auf den vollständigen Auskunftsanspruch, also auf alle gespeicherten Daten, Zweck- und Rechtsgrundlage, Herkunft und Empfängerkreis?
- Wird bei einem Auskunftsverlangen in hinreichender Weise sichergestellt, dass der Anfragende zur Erteilung der Auskunft berechtigt ist?
- Wenn diese Personendaten an den Anfragenden übermittelt werden, erfolgt dabei eine Prüfung der Identität des Anfragenden und eine Protokollierung der Übermittlung?

2. Recht auf Berichtigung unrichtiger Daten

- Sobald die Unrichtigkeit von Personendaten festgestellt wird, werden diese unverzüglich korrigiert?
- Gibt es eine automatisierte Berichtigungsbearbeitung?
- Ist sichergestellt, dass auch die Empfänger vorangegangener Datenübermittlung über diese Berichtigung in Kenntnis gesetzt werden?

3. Recht auf Löschung bzw. Sperrung personenbezogener Daten

- Werden Personendaten auf Verlangen der betroffenen Person vollständig und irreversibel gelöscht?
- Nach welchen Zeiträumen werden diese Daten gelöscht?
- Ist sichergestellt, dass die zunächst gelöschten Daten nicht wieder hergestellt werden können?

- Ist sichergestellt, dass an Empfänger vorangegangener Datenübermittlungen diese Löschungen weitergeleitet werden?
- Sofern an die Stelle einer Löschung der Daten eine Sperrung tritt, weil der Löschung ein Hindernis entgegen steht, muss gewährleistet sein, dass diese gespeicherten Personendaten gekennzeichnet werden, um ihre weitere Verarbeitung oder Nutzung einzuschränken.
- Gibt es eine Möglichkeit, die Datensätze so zu kennzeichnen, dass sie zwar gespeichert bleiben, aber nicht im Rahmen der normalen Verarbeitung genutzt werden?
- Wird diese Sperrung durch ein hinreichendes Verfahren gewährleistet?
- Gibt es eine Protokollierung sowohl hinsichtlich des Zeitpunkts aber auch des Auftraggebers bzgl. der Sperrung sowie auch ggf. eine Aufhebung dieser Sperre?

4. Widerspruchsrechte der Betroffenen

Dem Nutzer steht ein Widerspruchsrecht gegen die Bearbeitung seiner Daten zu. Auf einen Widerspruch des Betroffenen muss die weitere Bearbeitung seiner Personendaten unterbleiben, sofern die schutzwürdigen Interessen des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der datenbearbeitenden Stelle überwiegen.

- Ist gewährleistet, dass ein solcher Widerspruch unverzüglich berücksichtigt wird?
- Wird gewährleistet, dass nach erfolgtem Widerspruch die entsprechenden Daten umgehend gelöscht werden?
- Ist sichergestellt, dass solche Widersprüche auch am Empfänger vorangegangener Datenübermittlungen weitergeleitet werden?

5. Weiterleitungs- und Unterrichtungspflicht

Wenn mehrere Stellen zur Speicherung der Personendaten eines Nutzers berechtigt sind, sind diese Stellen verpflichtet, etwaige Anfragen eines Nutzers, an diejenige Stelle, die die Daten tatsächlich gespeichert hat, weiterzuleiten. Darüber hinaus ist auch der Nutzer über diese Weiterleitung des Vorbringens und auch über die

zuständige Stelle zu unterrichten.

- Falls derartige Anfragen einer betroffenen Person eingehen, muss gewährleistet sein, dass diese unverzüglich an die Stelle, die die Daten tatsächlich gespeichert hat, weitergeleitet werden. Ist dies der Fall?
- Ist gewährleistet, dass auch die betroffene Person über diese Weiterleitung ihrer Anfrage sowie auch die zuständige Stelle umgehend unterrichtet wird?

IV. Datenschutzmanagement

Die Gesamtorganisation des Dienstleistungserbringers berücksichtigt die Belange des Datenschutzes, so dass in den organisatorischen Abläufen, hinreichende Standards und Regelungen vorhanden sind, die die Erreichung der Datenschutzziele gewährleisten.

1. Datenschutzverantwortlicher

Das Unternehmen des Dienstleistungserbringers ernennt einen betrieblichen bzw. externen Datenschutzverantwortlichen, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt (Art. 11a Abs. 5 lit. e DSG).

- Ist ein Datenschutzbeauftragter wirksam bestellt worden?
- Kann der Datenschutzbeauftragte seine Funktion fachlich unabhängig ausüben?
- Hat der Datenschutzbeauftragte Zugang zu allen Datensammlungen und Datenbearbeitungen sowie zu allen Informationen, die er zur Erfüllung seiner Aufgabe benötigt?
- Ist eine Liste über die nicht angemeldeten Datensammlungen verfügbar?

2. Auftragsdatenbearbeitung

Sobald die Bearbeitung von Personendaten an Dritte ausgelagert wird oder Dritte bei der Bearbeitung beiziehen, liegt eine Auftragsdatenbearbeitung vor (beispielsweise Outsourcing, Cloud Computing, Hosting, Archivierung, Backup-Dienstleistungen, Speicherung von Personendaten auf fremden Servern, oder andere Arten von Dienstleistungsverträgen, die eine Auftragsdatenbearbeitung nach sich ziehen, weil der beauftragte Dritte zur Erbringung seiner Dienstleistungen mit Personendaten arbeitet, die vom Dienstleistungserbringer zur Verfügung gestellt werden). Die Übertragung der Datenbearbeitung an einen Dritten darf die Rechtsstellung der betroffenen Personen nicht verschlechtern.

- Erfolgt eine Datenbearbeitung durch einen beauftragten Dritten?
- Ist eine derartige Datenbearbeitung durch ein Drittunternehmen zulässig? (Art. 10a DSG)

- Ist ein entsprechender Auftragsdatenbearbeitungsvertrag abgeschlossen worden?
- Sind in diesem Vertrag die nach Art. 10a Abs. 1 lit. a und Abs. 2 DSG festzulegenden Einzelheiten bestimmt worden?
- Gibt es hinreichende technische und organisatorische Maßnahmen, die insbesondere auch die Bindung des beauftragten Dritten an die Weisungen des Dienstleistungserbringers gewährleisten?
- Hat der Dienstleistungserbringer den beauftragten Dritten sorgfältig ausgewählt, instruiert und überwacht er diesen und wird die sorgfältige Auswahl, Instruktion und Überwachung des beauftragten Dritten entsprechend dokumentiert?
- Sind die hinreichenden technischen und organisatorischen Maßnahmen auf ihre Einhaltung überprüft worden und wurde das Ergebnis der Prüfung dokumentiert?

3. Technische und organisatorische Sicherheitsmaßnahmen

Der Dienstleistungserbringer muss darlegen, dass in seinem Unternehmen die Personendaten durch angemessene technische und organisatorische Maßnahmen im Sinne von Art. 7 DSG i.V.m. Art. 8 DSV gegen unbefugtes Bearbeiten geschützt sind. Erforderlich sind solche Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Da es sehr unterschiedliche Gestaltungsmöglichkeiten hinsichtlich der Erreichung der Mindeststandards gibt, sind die nachfolgenden Fragen lediglich als Indiz bzw. Beispiele dafür zu verstehen, dass diese Schutzziele erfüllt werden.

a) Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen Personendaten verarbeitet oder genutzt werden, zu verwehren, wobei der Begriff räumlich zu verstehen ist.

- Zutrittskontrollsystem, Ausweisleser, Magnetkarte, Chipkarte etc.
- Schlüssel / Schlüsselvergabe
- Alarmsicherung, Türsicherung (elektrische Türöffner usw.)
- Werkschutz, Pförtner
- Überwachungseinrichtung wie z.B. Alarmanlage, Video-/Fernsehmonitor
- Zugangsprotokolle

b) Personendatenträgerkontrolle:

Unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen.

- Verschlüsselung von Datenträgern
- Verschlüsselung von Daten (auf Datenträgern)
- Richtlinien für den Umgang mit Datenträgern und/oder der sich darauf befindlichen Daten
- Nummerierung und Inventarisierung von Datenträgern,
- Kopierkontrolle
- fachgerechte Entsorgung nicht mehr benötigter Datenträger
- Informationsträger in Papierform: zentrale Druck- und Kopiersysteme mit Kontrollfunktion, fachgerechte Entsorgung durch Aktenvernichtung

c) Benutzerkontrolle

Unbefugten ist das Eindringen in bzw. Nutzen von Datenverarbeitungssysteme(n) untersagt. Zu diesem Zweck sind technische (Kennwort- / Passwortschutz) und

organisatorische (Benutzerstammsatz) Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung vorzusehen.

- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
- Zugriff auf Server nur mit persönlichem Konto und speziell definierten Zugangsrechten (Nutzergruppen)
- Verschlüsselung von Datenträgern bzw. Datenverkehr zwischen den Servern
- Vergabe von Admin-Accounts
- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte), z.B. durch Rechteverwaltung; nur befugte Personen haben Zugang zu den Serversystemen;
- Benutzer- und Rechteverwaltung nur durch klar definierte Mitarbeiter der IT

d) Zugriffskontrolle

Unerlaubte Tätigkeiten in Datenverarbeitungssystemen außerhalb eingeräumter Berechtigungen sind zu verhindern durch bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung.

- Differenzierte Berechtigungen (Profile, Rollen, Transaktionen und Objekte), z.B. durch Rechteverwaltung und Zugriffskontrolle
- Einrichtung eines Benutzerverwaltungssystems, betriebsinterne Chinese Walls
- Benutzer- und Rechteverwaltung nur durch klar definierte Mitarbeiter der IT
- Einsatz von professionellen und sicheren Archivierungslösungen
- Zuverlässige Löschung von Daten bzw. Datenträgern

e) Weitergabekontrolle (Transportkontrolle)

Die Aspekte der Weitergabe personenbezogener Daten sind zu regeln, z.B. hinsichtlich der elektronischen Übertragung, Datentransport, Übermittlungskontrolle, etc. Dazu zählen auch Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung.

- Absicherung der elektronischen Kommunikationswege, z.B. durch Einrichten von geschlossenen Netzwerken oder Verfahren zur Verschlüsselung von zu übertragenden Daten

- Tunnelverbindung (VPN = Virtual Private Network)
- Elektronische Signatur
- Protokollierung
- Transportsicherung, z.B. durch Verwendung von sicheren Transportbehältern für Datenträger

f) Bekanntgabekontrolle

Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können.

- Protokollierung
- Authentifizierung von Adressdaten

g) Eingabe- und Speicherkontrolle

Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten, z.B. durch Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind.

Unbefugte Eingaben, Einsichtnahme oder Veränderung durch unberechtigte Personen sollen verhindert werden.

- Detaillierte Protokollierungs- und Protokollauswertungssysteme hinsichtlich der Erstellung, Veränderung und Entfernung von Datensätzen
- Berechtigungssysteme
- Fernlöschungsmechanismen (bspw. bei Abhandenkommen eines Endgeräts)

h) Auftragskontrolle

Soweit eine Auftragsdatenbearbeitung i.S.v. Art. 10a DSG gegeben ist: Der Dienstleistungserbringer muss sich vergewissern, dass der Dritte die Datensicherheit gewährleistet. Insbesondere ist durch Maßnahmen (technisch sowie organisatorisch) zur Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer die weisungsgemäße Auftragsdatenbearbeitung zu gewährleisten.

- Eindeutige Vertragsgestaltung
- Formalisierte und damit standardisierte Erteilung von Aufträgen (Auftragsformular) bzw. Weisungen
- Kriterien zur Auswahl des Auftragnehmers
- Klare Kompetenzabgrenzungen

- Kontrolle der Vertragsausführung
- Einforderung der Einhaltung von Standards und Nachweis durch Zertifikate

i) Datenintegrität

Es ist sicherzustellen, dass die Personendaten vollständig, gültig und aktuell sind.

- Systemwartung
- Schutz vor Malware / Firewall

j) Verfügbarkeitskontrolle

Es ist sicherzustellen, dass die Personendaten auf Anfrage einer berechtigten Stelle zugänglich und benutzbar sind. Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen durch physikalische bzw. logistische Maßnahmen zur Datensicherung.

- Backup-Verfahren
- Spiegeln von Festplatten, z.B. RAID-Verfahren
- Regelmäßige Erstellung von vollwertigen Sicherungskopien und deren Auslagerung an anderen Ort
- Regelmäßiges Testen der Datenwiederherstellung
- Unterbrechungsfreie (akkugestützte) Stromversorgung
- Erstellung eines Notfallkonzepts und entsprechender schriftlicher Unterlagen

k) Trennungskontrolle

Daten, die zu unterschiedlichen Zwecken erhoben wurden, sind auch getrennt zu verarbeiten. Daher sind Maßnahmen zur getrennten Verarbeitung (Speicherung, Veränderung, Löschung, Übermittlung) von Daten mit unterschiedlichen Zwecken zu gewährleisten.

- Vergabe von Zugriffsberechtigungen/-beschränkungen
- Verschlüsselte Speicherung von Personendaten, damit diese im Falle eines versehentlichen Abrufs durch Dritte nicht von diesen gelesen werden können
- Speicherung auf physikalisch getrennten Systemen (Trennung nach Kompetenzen und Aufgabengebieten)

4. Innerbetriebliche Regelungen

Der Lizenzberechtigte muss darlegen, dass er den Umgang mit Daten im Betrieb aktiv führt (Datenschutzmanagement) und in seinem Unternehmen hinreichende innerbetriebliche Regelungen, insbesondere auch für die Mitarbeiter, zum Thema Datenschutz existieren.

- Sind alle mit der Datenbearbeitung beschäftigten Mitarbeiter auf die Geheimhaltung von Daten, und gegebenenfalls die Einhaltung von Geschäfts- oder Berufsgeheimnissen verpflichtet worden?
- Sind in den Unternehmen systematische Regelungen zum Umgang mit Personendaten bzw. besonders schützenswerten Daten vorhanden?
- Sind für die Mitarbeiter Anweisungen vorhanden für die zum Thema Daten- und Geheimnisschutz aufkommenden Fragen?
- Werden die Mitarbeiter in regelmäßigen Abständen für das Thema Daten- und Geheimnisschutz sensibilisiert bzw. finden in regelmäßigen Abständen entsprechende Schulungen statt?
- Prüft der Dienstleistungserbringer periodisch im Rahmen der betrieblichen Risikoanalyse die IT Sicherheit und die Konformität des Datenschutzmanagements in Bezug auf die Datenschutzvoraussetzungen?
- Hat der Dienstleistungserbringer für den Fall der Nichtkonformität Prozesse definiert (gesamter Prozess der Identifikation, der Analyse und der Bewertung der Nichtkonformität sowie den Umgang mit der Nichtkonformität)?