Technische und Organisatorische Maßnahmen (DSGVO)

- Vertraulich-

Weitergabe an Dritte oder Veröffentlichung nicht gestattet

INFOnline GmbH
Brühler Straße 9
53119 Bonn

Tel.: +49 228 410 29 -0
Fax: +49 228 410 29 -66

http://www.infonline.de
info@infonline.de

Inhaltsverzeichnis

1. Grundlagen

1.1. Vorbemerkung

In diesem Dokument werden die bestehenden technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO bei der INFOnline GmbH (im Folgenden „INFOnline“) beschrieben.

Die in diesem Dokument enthaltenen Informationen sind als vertraulich klassifiziert und dürfen ohne die schriftliche Genehmigung von INFOnline keinem Dritten zugänglich gemacht werden.

1.2. Ziel dieses Dokuments

Die vorliegenden Informationen zum Thema Datenschutz und Datensicherheit bei INFOnline geben einen Überblick über die Grundbausteine des Datenschutz- und Sicherheitskonzepts und erläutern die technischen und organisatorischen Maßnahmen im Hinblick auf den von INFOnline angebotenen Service SZMnG.

1.3. Unternehmensbeschreibung

1.3.1. INFOnline

Seit 2002 misst INFOnline die Seitenzugriffe auf Digital-Angebote nach den einheitlichen Standards der Arbeitsgemeinschaft Online-Forschung (agof) und der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (im Folgenden „IVW“).

Diese von INFOnline ermittelten Leistungswerte werden von der IVW und der agof dazu verwendet, die Vermarktung des Mediums "Online" in Deutschland auf der Basis von vergleichbaren, geprüften und vertrauenswürdigen Daten zu ermöglichen.

Als zentraler Ansprechpartner für die Mitglieder der IVW bietet INFOnline neben der technischen Messung auch einen umfangreichen Service für die Angebotsbetreiber zu technischen, organisatorischen und vertraglichen Fragen an.

Die technische Messung erfolgt mit dem **Skalierbaren Zentralen Messverfahren („SZMnG“)**. Kunden von INFOnline können ihre gemessenen Leistungswerte (u.a. Page Impressions, Visits, im Folgenden „PI(s)/Visits“) über ein Auswertewerkzeug analysieren.

1.3.2. IVW

Die IVW ermittelt und prüft seit 1949 neutral und objektiv die Verbreitung von Werbeträgern. Da das Medium Online in den letzten Jahren ein nicht wegzudenkender Träger von Werbebotschaften ist, nutzt die IVW die Messergebnisse aus dem SZMnG-Verfahren, um im Rahmen einer eigenen nachträglichen Prüfung die durch das SZMnG gezählten Zugriffe (PIs und

Visits) auf zuvor kategorisierte Webseiten ihrer Verbandsmitglieder, die allesamt gleichzeitig Kunden von INFOnline sind, stichprobenartig nachvollziehen zu können. Daneben prüft die IVW die Einhaltung der zugrunde liegenden Richtlinien für die Online-Zählung und veröffentlicht monatlich Page Impressions und Visits ihrer Mitgliedsangebote. Hintergrund der gewählten Konstellation ist, dass die IVW sowie die angeschlossenen Medienanbieter, Werbetreibenden und Werbeagenturen ein effektives Kontrollsystem aufrechterhalten möchten, das unter einer gemeinsamen Aufsicht (IVW) steht.

1.3.3. agof

Die agof wurde im Dezember 2002 von Online-Vermarktern und -Werbeträgern gegründet. Der Zusammenschluss dient dazu, gemeinsam eine kontinuierliche Onlineforschung gemäß etablierter Marktstandards zu erarbeiten, durchzuführen und weiterzuentwickeln. Dies schließt die Erhebung, Auswertung und Vermarktung von erstellten Daten, Studien und Forschungsergebnissen ein. Die agof strebt im Rahmen dieser Onlineforschung die konsensuelle Ermittlung von Daten zur Nutzung und Werbeträgerleistung von Online-Diensten und Digital-Angeboten an.

Die kontinuierliche Onlineforschung richtet sich methodisch an den folgenden Eckpfeilern aus:

- kontinuierliche Telefonbefragung,
- OnSite-Befragung,
- Technische Messung durch das SZMnG / INFOnline

1.4. Ansprechpartner

1.4.1. EDV, IT-Sicherheit

INFOnline GmbH
Brühler Straße 9
D-53119 Bonn

Steffen Passmann
CTO (Chief Technology Officer)

Thomas Gray
IT-Sicherheitsbeauftragter

1.4.2. Datenschutzbeauftragter

SICODA GmbH
Rochusstraße 198
D- 53123 Bonn

Peter Mühlemeier
Datenschutzbeauftragter

1.5. Verfahrensbeschreibung

1.5.1. Beschreibung

Das SZMnG basiert im Wesentlichen darauf, dass durch technische Maßnahmen einzelne Zugriffe auf die Webseiten oder innerhalb von Smartphone-Applikationen der Kunden

- erfasst,
- abgegrenzt,
- gezählt

werden können.

Die durch die Messung erhobenen Daten werden abhängig vom Auftrag aggregiert und regelmäßig an die IVW e.V. und agof e.V. weitergeleitet, die diese anschließend prüfen und veröffentlichen.

Damit die Zugriffe einer Webseite durch INFOnline gemessen werden können, muss durch den Kunden (Betreiber der Webseite) ein Javascript-Code implementiert werden. Für die Messung der

mobilen Nutzung stellt INFOnline für verschiedene Plattformen eine Mess-Library zur Verfügung, die von den Kunden / Entwicklern in die eigenen Applikationen implementiert werden kann. Bei der Nutzung der gemessenen Webseiten oder Applikationen wird ein Zählimpuls an das SZMnG der INFOnline gesendet.

Die erhobenen Daten ermöglichen aufgrund der Datenarten und Datenmenge keine eindeutige Identifizierung eines Nutzers als Person.

1.5.2. SZMnG

Damit die Nutzung einer Webseite technisch gemessen werden kann, muss durch den Kunden ein Javascript-Code im HTML-Quellcode (SZMnG-Tag) implementiert werden. Der Aufruf dieses Javascripts über den Browser bzw. das Endgerät des Nutzers (Client) löst die Messung im SZMnG aus und ggfs. die Auslieferung einer Einladung zur Teilnahme an einer Online-Befragung.

Das System zur Online-Befragung wird nicht durch INFOnline betrieben, es erfolgt lediglich eine Weiterleitung auf dieses System.

Soll die Nutzung einer Smartphone/Tablet-Applikation gemessen werden, so wird durch den Anbieter der Applikation eine Software-Library eingebunden, die INFOnline zur Verfügung stellt. Die Library stellt sicher, dass alle benötigten Informationen im richtigen Format an das Messsystem übermittelt werden.

Die an INFOnline übermittelten Zählimpulse werden zunächst als Rohdaten temporär zwischengespeichert und die IP-Adressen anonymisiert. Die Anonymisierung durch Kürzung der IP-Adressen erfolgt dabei frühestmöglich (Bei IPv4 Kürzung um 1 Byte). Sonstige eindeutige Identifier von Endgeräten werden ausschließlich als Hash übertragen.

INFOnline bietet die Möglichkeit eines Opt-Out (https://optout.ioam.de) aus der Messung.
Die Aktivierung des Opt-Outs in einem Webbrowser führt dazu, dass die Zählimpulse des Browsers im Messsystem verworfen werden. Es erfolgt in diesem Fall keine weitergehende Analyse oder Messung der Zählimpulse dieses Browsers.
Die Implementierung des Opt-Outs in Applikationen obliegt dem jeweiligen Anbieter der App. INFOnline beschreibt im jeweiligen Integration Guide der verschiedenen Plattformen, wie das Opt-Out in Applikationen umgesetzt werden kann.

Beispiele der erhobenen Daten:

Zeitstempel, IP-Adresse (gekürzt), Cookie-Inhalt, aufgerufene Webseite, Signatur des Browsers, ID des Endgerätes als Hash (bei Smartphones), ausgelöstes Event (z.B. „start“,“stop“) usw.

In den nachgelagerten Systemen werden die Daten analysiert und gespeichert.

Die aggregierten und ausgewerteten Messdaten werden über definierte Schnittstellen für die IVW e.V. und agof e.V. bereitgestellt. Hierzu steht eine im Internet verfügbare standardisierte Schnittstelle zur Verfügung. Die Übertragung der Daten erfolgt dabei stets verschlüsselt.

1.5.2.1. Export für IVW

Die Messwerte der einzelnen Angebote, die Mitglied bei der IVW sind, werden regelmäßig an die IVW übermittelt (Online-Schnittstelle, verschlüsselte Übertragung).

Der Export enthält Page Impressions, Visits, Kategorien, Themen und die Daten der Inlands-/ Auslandsnutzung der gemessenen Angebote.

1.5.2.2. Export für agof

INFOnline liefert regelmäßig die für die agof-Studien benötigten Messdaten (Online-Schnittstelle, verschlüsselte Übertragung).

Der Export enthält die Bewegungsdaten inkl. der Client-Identifier der Geräte/Browser, welche sich in einer regelmäßig erhobenen Stichprobe befinden.

2. Organisationskontrolle

Werden Daten automatisiert verarbeitet oder genutzt, ist die innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

2.1. Gesetzliche Grundlagen

Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gelten die Vorschriften der Datenschutzgrundverordnung (DSGVO) bzw. des BDSG-neu.

Insbesondere sind für die Datenverarbeitung im Auftrag durch INFOnline folgende Regelungen zu beachten:

▪ Art. 37 DSGVO	Beauftragter für den Datenschutz
▪ Art. 39 DSGVO	Aufgaben des Beauftragten für den Datenschutz
▪ Verpflichtung auf Vertraulichkeit	
▪ Art. 32 DSGVO	Technische und organisatorische Maßnahmen
▪ Art 28 ff. DSGVO	Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag
▪ Art. 51. ff. DSGVO	Aufsichtsbehörde
▪ Art 83 DSGVO	Bußgeldvorschriften
▪ §84 BDSG (neu)	Strafvorschriften

2.2. Beauftragter für den Datenschutz

Gemäß Art. 37 DSGVO hat INFOnline einen betrieblichen Datenschutzbeauftragten zu bestellen. Die Aufgabe des betrieblichen Datenschutzbeauftragten wird für INFOnline intern durch den unter 1.4.2 genannten Datenschutzbeauftragten wahrgenommen.

2.3. Formale Voraussetzungen und Maßnahmen

2.3.1. Verzeichnis von Verarbeitungstätigkeiten

Im Rahmen der Verarbeitung personenbezogener Daten sowie bei der Verarbeitung von aggregierten internen Kennungen im SZMnG-Verfahren führt INFOnline ein Verzeichnis aller Verarbeitungstätigkeiten, die der Zuständigkeit von INFOnline unterliegen (Art. 30 Abs. 1 DSGVO). Als Auftragsverarbeiter führt INFOnline ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung (Art. 30 Abs. 2 DSGVO).

Das Verzeichnis gem. Art. 30 Abs. 1 DSGVO enthält sämtliche folgenden Angaben:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
2. die Zwecke der Verarbeitung;
3. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
4. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
5. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
6. wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
7. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Dabei dokumentiert INFOnline auf der Ebene der Verarbeitung bzw. des Verfahrens eine Reihe weiterer Umstände. Dies betrifft z.B. bestehende Zugriffsberechtigungen.

Die für INFOnline vorliegende Übersicht wird im Rahmen regelmäßiger Statusgespräche bei Bedarf aktualisiert.

2.3.2. Auftragsverarbeitung

INFOnline erbringt die Dienstleistung der Messung von Webseiten-Zugriffen gegenüber ihren Kunden regelmäßig als Auftragsverarbeitung gemäß Art. 28 DSGVO.

2.3.3. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass die Verarbeitung personenbezogener Daten im Auftrag (z.B. durch ein Rechenzentrum) nur nach den Weisungen des Auftraggebers erfolgt. Insbesondere sind im Vertrag die Art und Weise der Auftragserteilung zu formalisieren.

2.3.3.1. Im SZMnG

Die mit den Auftraggebern zu schließenden Verträge zur Auftragsverarbeitung enthalten Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung der Daten des Auftraggebers.

2.4. Innerbetriebliche Organisation

2.4.1. Personelle Maßnahmen

2.4.1.1. Verpflichtung auf Vertraulichkeit

Alle Mitarbeiter von INFOnline werden auf Vertraulichkeit verpflichtet.

Neben einer allgemeinen Aufklärung über die Bedeutung der Vertraulichkeit enthält diese Verpflichtung auch Hinweise auf weitergehende Informationen zum Datenschutz sowie auf eventuelle Sanktionen.

2.4.1.2. Weitergehende Verpflichtungen

Soweit Mitarbeiter mit der Wartung der unternehmenseigenen EDV oder Telekommunikationsanlage betraut sind, werden diese auf die Wahrung des Fernmeldegeheimnisses nach § 88 TKG verpflichtet.

2.4.1.3. Information und Schulung

Die bei INFOnline geltenden Regelungen zu Datenschutz, IT-Sicherheit und Informationsschutz sind in entsprechenden Richtlinien für den datenschutzkonformen Einsatz der Informations- und Kommunikationstechnik allen Mitarbeitern zugänglich.

Erste Informationen zu geltenden Regelungen zu Datenschutz, IT-Sicherheit und Informationsschutz erhalten die Mitarbeiter bereits bei Einstellung im Arbeitsvertrag. Weitergehende Informationen folgen im Zusammenhang mit der schriftlichen Verpflichtung auf Vertraulichkeit sowie im Rahmen der arbeitsplatzbezogenen Einweisung.

Hierdurch wird sichergestellt, dass jeder Mitarbeiter über folgende Punkte informiert ist:

- Grundlagen des Datenschutzes
- Interne Regelungen zum Datenschutz, IT-Sicherheit und Informationsschutz

- Grundzüge technischer und organisatorischer Maßnahmen zur Sicherstellung von Datenschutz, IT-Sicherheit und Informationsschutz
- Verantwortlichkeiten
- Informationsquellen

Ergänzend zu diesen grundsätzlichen Informationen werden die Mitarbeiter im Rahmen der monatlichen Team-Meetings tiefergehend im Hinblick auf spezielle Datenschutzfragen und deren Anwendung bei INFOnline informiert. Darüber hinaus veröffentlicht der Datenschutzbeauftragte von INFOnline regelmäßig Datenschutz-News im INFOnline-Portal.

Durch das dargestellte Konzept wird sichergestellt, dass sowohl neu eingestellte Mitarbeiter in die Thematik des Datenschutzes eingeführt werden als auch die Kenntnisse der schon länger bei INFOnline beschäftigten Mitarbeiter regelmäßig aufgefrischt und aktualisiert werden.

Im Übrigen ist der eigentliche Verarbeitungsvorgang von Auftragsdaten durch rechtskonform zu gestaltende Weisungen des Auftraggebers vorgegeben, da der Umgang mit Daten regelmäßig weisungsgebunden im Rahmen eines Auftragsverhältnisses nach Art. 28 DSGVO erfolgt.

Auf Ebene der Datensicherheit bestehen zusätzliche Schulungsmaßnahmen für Arbeiten auf EDV-Anlagen im Rechenzentrum. Mitarbeiter, die über Zugriff auf unternehmenskritische Systeme im Rechenzentrumsbetrieb verfügen, werden regelmäßig in systemrelevanten Fragen geschult und sind RHCT / RHCSA (RedHat Certified Technican / RedHat Certified Administrator) zertifiziert und/oder haben eine Ausbildung bzw. Studium im Bereich Informatik oder Elektrotechnik absolviert.

2.4.1.4. Regelmäßige Information

INFOnline erhält über den Datenschutzbeauftragten regelmäßig neueste Informationen über technische und rechtliche Entwicklungen auf den Gebieten des Datenschutzes und der Datensicherheit, so dass ständig eine entsprechende Sensibilisierung bei INFOnline gegeben ist.

2.4.1.5. Richtlinien

INFOnline verfügt über einen Richtlinien-Katalog hinsichtlich der Regelung datenschutzrechtlicher sowie sicherheitsrelevanter Themen. Beispielhaft seien hierzu aufgeführt:

- Zutrittsregelungen der Rechenzentren
- Zugriffsmanagement interne Systeme

2.4.2. Rechte der betroffenen Personen

In Fällen, in denen betroffene Personen anfragen, welche Informationen über sie verarbeitet werden, wird die Anfrage an den Datenschutzbeauftragten zur Prüfung und Koordination der Bearbeitung in Gestalt der Weitergabe an den verantwortlichen Auftraggeber weitergeleitet.

Ebenso verhält es sich bei der Geltendmachung von Rechten Betroffener auf Berichtigung, Löschung und Sperrung von Daten.

3. Sicherheitsgrundsätze bei INFOnline

Aus den gesetzlichen Vorgaben des Art. 32 DSGVO resultiert die Pflicht der datenschutzrechtlich verantwortlichen Stelle, die automatisierte Datenverarbeitung technisch und organisatorisch abzusichern. Damit einhergehend müssen Grundbedrohungen für die Verfügbarkeit, Integrität und Vertraulichkeit der Datenbestände erkannt und mit entsprechenden präventiven Maßnahmen versehen werden. Bei INFOnline bestehen daher in Bezug auf die Datenverarbeitung durch das SZMnG zugunsten der Auftraggeber als datenschutzrechtlich verantwortliche Stelle als Grundbasis drei Standardsicherheitsanforderungen, die als Sicherheitsschichten aufeinander aufbauen. Die äußerste Schicht bilden vor allem diejenigen Maßnahmen, die zur Abwehr eines unbefugten Zutritts bzw. Zugangs zu den im Bürobetrieb eingesetzten Datenträgern bzw. Datenträgersystemen dienen. Der Fokus ist auf die eingesetzten Datenträger gerichtet, weil ausschließlich auf ihnen personenbezogene Daten verarbeitet werden, die unter dem Schutz der DSGVO stehen.

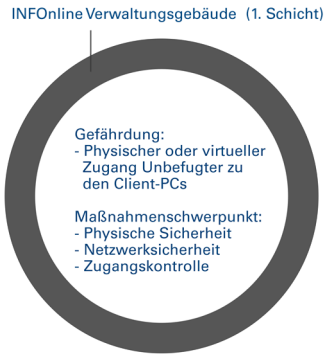
Eine zweite Sicherheitsschicht bildet der Rechenzentrumsbetrieb von INFOnline. Aufgrund der systemischen Ausgestaltung in eine Client- (Verwaltungsgebäude) und Serverumgebung (Rechenzentrum) vollzieht sich der Schwerpunkt der Datenverarbeitung im Rechenzentrum von INFOnline. Diesbezüglich müssen daher erhöhte Anforderungen an die Zutritts- und Zugangsbeschränkungen bestehen. Daneben bestehen im Rechenzentrumsbetrieb ebenfalls erhöhte Anforderung an die Verfügbarkeit und Integrität der dort gespeicherten Daten.

Werden die ersten beiden Sicherheitsschichten durch das für die Datenverarbeitung eingesetzte Personal auf legale Weise überwunden, muss im Weiteren verhindert werden, dass die in der zentralen Applikation (SZMnG) verarbeiteten Daten unbefugt zur Kenntnis genommen oder verarbeitet werden. Hierzu werden primär Zugriffsberechtigungen durch den IT-Service in der

Hauptverwaltung für die Server und EDV-Anlagen im Rechenzentrum anhand vorgegebener, rollen-basierter Profile vergeben.

In diesem Zusammenhang wird im Rahmen der befugten Betreuung der Applikation darauf geachtet, dass Nutzeraktivitäten im Nachhinein nachvollziehbar sind. Dies vollzieht sich durch eine wirksame Protokollierung von Nutzeraktivitäten und –eingaben.

3.1. Erste Sicherheitsschicht



Hauptbestandteil der ersten Sicherheitsschicht, die als Ring die übrigen inneren Sicherheitsbereiche in Gestalt des Rechenzentrums- und SZMnG-Betriebs einschließt, sind die Räumlichkeiten der Hauptverwaltung von INFOnline in Bonn, aus denen die wesentlichen Maßnahmen für den SZMnG-Betrieb koordiniert werden. Es erhält niemand, außer den explizit ausgewiesenen Mitarbeitern von INFOnline gemäß ihres Funktions- und Aufgabenbereichs, Zugang zu den Datenträgern in den Büroräumen.

Folglich wird diejenige Person per se als Unbefugter betrachtet, die nicht Mitarbeiter von INFOnline ist.

3.1.1. Physische Sicherheit (Zugangskontrolle)

Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Ziel der Zugangskontrolle ist es, zu gewährleisten, dass nur berechtigte Personen Zugang zu Grundstücken, Gebäuden, Bereichen und Räumen haben, in welchen sich Einrichtungen für die Datenverarbeitung (DV-Anlagen, Server, PCs/Terminals, Systemkomponenten usw.) befinden.

Die Räumlichkeiten von INFOnline, ausgenommen des Rechenzentrums, befinden sich in Bonn in einem Gebäudekomplex mit mehreren Parteien. INFOnline steht hierbei ein eigener Bereich mit gesonderter Schließvorrichtung zur Verfügung. Darüber hinaus sind die Räumlichkeiten von INFOnline alarmgesichert.

Besucher haben sich beim Empfang anzumelden und sind gehalten, nur in Begleitung eines Mitarbeiters von INFOnline die weiteren Büroräume zu betreten.

3.1.2. Speicherkontrolle und Benutzerkontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Ziel der Speicher- und Benutzerkontrolle ist es, durch technische Maßnahmen sicherzustellen, dass nur berechtigte Personen Zugang zu Rechnern, Servern, Systemkomponenten etc. haben. Dies gilt sowohl für die Inbetriebnahme als auch für den laufenden Betrieb.

3.1.2.1. Netzwerksicherheit

Als Zugang Unbefugter zu den Datenverarbeitungsräumen und Arbeitsplatzsystemen in der Hauptverwaltung wird bei INFOnline auch ein unberechtigter Authentifizierungsversuch aus dem Internet in das eigene interne Netzwerk verstanden. Derartige Zugriffe sind in Bezug auf die Räumlichkeiten von INFOnline und die dort betriebenen PCs nicht vorgesehen. Dort finden sich lediglich Client-Rechner und Netzwerkkomponenten. Eine eigens für die Büroräumlichkeiten eingesetzte Firewall sorgt dafür, dass die Vorgabe in Gestalt des Verbots von Zugriffen von außen wirksam durchgesetzt wird. Diese Firewall wird von den Systemspezialisten regelmäßig gewartet. Zusätzlich sind für die Administratoren abgewiesene Anmeldeversuche anhand erstellter Sicherheitsprotokolle jederzeit nachvollziehbar.

Sollten Mitarbeiter aus dem Unternehmen ausscheiden, werden die jeweiligen Benutzerkonten umgehend gesperrt.

3.1.2.2. PCs/Netzwerk

Als Benutzerkontrolle wird auf den PCs die Zugangskontrolle zum entsprechenden Betriebssystem verbunden mit der Zugangskontrolle zum Netz genutzt.

Vor der Benutzung der PCs müssen sich die Mitarbeiter durch die Eingabe einer Benutzerkennung und eines Passwortes im Netzwerk identifizieren und authentifizieren.

Damit auch bei einer kürzeren Abwesenheit des IT-Benutzers ein Zugriffsschutz für das IT-System gewährleistet ist, sind die Benutzer angehalten, die Bildschirmsperre zu aktivieren. Festplatten von Notebooks sind verschlüsselt.

3.1.2.3. Passwortverfahren

Durch die Anmeldung am Microsoft Active Directory und den dort hinterlegten Vorgaben hinsichtlich der Passwortsicherheit (Mindestlänge etc.) werden triviale Passwörter der Nutzer systemseitig als unzulässig eingestuft. Daneben werden bereits verwendete Passwörter bei der Änderung eines Passwortes nicht akzeptiert (Passworthistorie). Kennwörter werden darüber hinaus - je nach Sensitivität - als Administrator- oder Nutzerkennung regelmäßig geändert.

3.1.3. Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind bzw. dass die Daten dann zur Verfügung stehen, wenn sie benötigt werden.

3.1.3.1. Datensicherungskonzept

Die Datensicherung vollzieht sich in der zweiten Sicherheitsschicht von INFOnline, da eine lokale Datenhaltung auf den Client-PCs nicht vorgesehen ist. Datenspeicherungen erfolgen an zentraler

Stelle, die physisch auf einem File-Server in einem Rechenzentrum von INFOnline gehalten werden.

3.1.3.2. Virenkonzept

Sämtliche Arbeitsplatzsysteme sind durch eine aktuelle Virenschutzlösung gesichert. Hierbei überprüft die Antiviren-Software automatisch im Hinblick auf neue Viren-Signaturen und aktualisiert diese bei Bedarf.

Auf dem eingesetzten Mailserver werden eingehende E-Mails ebenfalls automatisch auf Viren überprüft. Infizierte E-Mails werden dem Empfänger nicht zugestellt, sondern verbleiben zur Löschung durch den Administrator in einem geschützten Speicherbereich.

3.1.4. Datenträgerkontrolle von beweglichen Datenträgern

Es ist zu gewährleisten, dass personenbezogene Daten während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

3.1.4.1. Bewegliche Datenträger

Das Datenträgerschutzkonzept für bewegliche Datenträger im Haus von INFOnline gliedert sich in zwei Bereiche: Zum einen befasst es sich mit Datenträgern und deren Inhaltsschutz, solange diese noch benötigt werden. Zum anderen wird über dieses Konzept die Entsorgung der Datenträger, die nicht mehr benötigt werden oder defekt sind, geregelt. Als bewegliche Datenträger werden Festplatten, USB-Sticks, Bänder, CDs und DVDs definiert.

Die Festplatten in sämtlichen mobilen Geräten sind verschlüsselt. Zugang zu derart geschützten Datenträgern wird nur nach korrekter Eingabe von Benutzernamen und Kennwort gewährt.

Sollten Datenträger nicht mehr benötigt werden, stehen Software-Tools zum sicheren Löschen der Daten bereit.

Muss ein defekter Datenträger entsorgt werden, so wird dieser einem zertifizierten (ISO 9001, EfbV) Dienstleister zur Vernichtung übergeben.

3.1.5. Allgemeines Berechtigungskonzept (Organisation)

Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Ziel der Zugriffskontrolle ist es, über ein Berechtigungskonzept sicherzustellen, dass der Zugriff auf personenbezogene Daten nur in dem Umfang ermöglicht wird, wie es für die jeweilige Aufgabenerledigung erforderlich ist. Aus dem Berechtigungskonzept muss zweifelsfrei

hervorgehen, welche Benutzer auf welchen Benutzer(gruppen) auf welche Daten, Funktionen, Objekte usw. Zugriff haben.

Die Organisation der Berechtigungsvergabe für die einzelnen Applikationen vollzieht sich bereits in der ersten Sicherheitsschicht in den Räumlichkeiten von INFOnline.

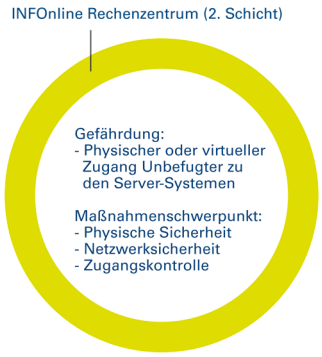
Hierbei werden die Berechtigungen einzelner Mitarbeiter von INFOnline sowohl im Rahmen der verfügbaren IT-Applikationen als auch bei den Regelungen zur Zutrittskontrolle in den Räumlichkeiten von INFOnline zentral koordiniert. Hierdurch kann bestmöglich gewährleistet werden, Berechtigungen nur nach dem jeweiligen Aufgabengebiet der Mitarbeiter zu verteilen.

Darüber hinaus bekommt jedes Benutzerkonto standardmäßig nur minimale Berechtigungen, die für die Durchführung der Tätigkeiten des Mitarbeiters benötigt werden.

INFOnline dokumentiert die Zugriffsrechte pro Server/System.

Eine Veränderung der Berechtigungen bedarf der schriftlichen Beantragung. Die Personalabteilung informiert darüber hinaus zeitnah den Bereich der Benutzerverwaltung über personelle Veränderungen in Textform. Dies gilt auch im Hinblick auf z.B. Aushilfen, Praktikanten und andere temporär Beschäftigte.

3.2. Zweite Sicherheitsschicht



Den Schutzbereich der zweiten Sicherheitsschicht bildet das Rechenzentrum von INFOnline. In diesem Umfeld bedarf es besonderer Sicherheitsvorkehrungen, die den Zugang Unbefugter auf die dort vorgehaltenen Informationen verhindern können.

Darüber hinaus bedarf es aufgrund der physischen Datenhaltung – im Gegensatz zu den Verwaltungs-räumlichkeiten von INFOnline – besonderer technischer und organisatorischer Maßnahmen zur Gewährleistung einer ausreichenden Verfügbarkeit der dort verarbeiteten Daten der Auftraggeber.

3.2.1. Physische Sicherheit (Zugangskontrolle)

3.2.1.1. Rechenzentrum Bonn

INFOnline unterhält insgesamt zwei Rechenzentren. Das Hauptrechenzentrum befindet sich in Bonn (im Folgenden „RZBN“). In diesem für die Datenhaltung und den Datentransfer im Bereich der Kreditwirtschaft zertifizierten Rechenzentrum unterhält INFOnline einen eigenen durch Zäune abgetrennten und abgeschlossenen Bereich („Cage“) mit einer eigenen Serverinfrastruktur sowie einer eigenen mehrfach redundanten Internetanbindung.

Es erhalten nur Personen Zutritt, deren Name beim Betreiber hinterlegt ist und die über eine persönliche Chipkarte verfügen. INFOnline selbst führt dabei eine gesonderte Übersicht, welcher Mitarbeiter von welcher Abteilung Zutritt zum Rechenzentrum bekommen soll.

Betritt der befugte Mitarbeiter von INFOnline die Räumlichkeiten des Rechenzentrums, dokumentiert das dortige Zutrittskontrollsystem automatisch, zu welchem Zeitpunkt mit welcher Chipkarte eine Türe geöffnet wurde. Darüber hinaus werden Zutritte zum Cage von INFOnline videoüberwacht.

Ist es erforderlich, Mitarbeitern von Wartungsfirmen zum Zwecke der Wartung von Spezialsystemen Zugang zum Rechenzentrum zu gewähren, geschieht dies nur in Begleitung eines Mitarbeiters von INFOnline. Im Eingangsbereich des Rechenzentrums wird der Name des Wartungsbesuches mit einer Datums- und Zeitangabe schriftlich festgehalten und mit Unterschrift bestätigt. INFOnline hat bei Bedarf Zugriff auf das vorgehaltene Protokoll.

3.2.1.2. Rechenzentrum Düsseldorf

Zutritt zum Rechenzentrum in Düsseldorf (im Weiteren „RZDUS“) wird ebenfalls nur denjenigen Personen gewährt, deren Name und Ausweisnummer beim Betreiber des Rechenzentrums hinterlegt sind. Vor einem Besuch des Rechenzentrums haben sich selbst registrierte zugangsberechtigte Personen beim Betreiber telefonisch anzumelden. Die registrierten Ausweisdokumente werden durch Sicherheitspersonal im Eingangsbereich überprüft. Der Bereich von INFOnline ist videoüberwacht.

3.2.2. Benutzerkontrolle

3.2.2.1. Rechenzentrum Bonn

a. **Netzwerk/Applikation**

Neben den allgemeinen Authentifizierungsmechanismen bei Benutzung der Client-PCs in den Büroräumen von INFOnline besteht im Rahmen des Rechenzentrumsbetriebs eine weitere Zugangskontrolle für legitimierte Mitarbeiter von INFOnline, die mit der technischen und fachlichen Betreuung der dort betriebenen Applikationen, so auch das SZMnG, von außen, d.h. ohne physischen Zugang zu den Servern im Rechenzentrum, befasst sind. Hierzu wird jeweils ein gesondertes Benutzerkonto durch die Benutzerverwaltung von INFOnline eingerichtet.

Der Zugriff von extern, zu dem auch ein Zugriff aus den Räumlichkeiten von INFOnline gewertet wird, ist dabei nur per VPN-Tunnel möglich. Ein direkter Zugriff auf einzelne Maschinen im internen Netz ist von „außen“ nicht möglich.

b. **Passwortverfahren**

Das Passwortverfahren für externe Zugriffe auf die im Rechenzentrum betriebenen Maschinen entspricht den Vorgaben in der unternehmenseigenen Passwortrichtlinie für die Hauptverwaltung.

c. **Externe Zugangsmöglichkeiten**

Es bestehen für die IVW e.V. und agof eingeschränkte externe Zugangsmöglichkeiten auf bestimmte Datenverarbeitungsvorgänge im Rechenzentrum.

aa. **IVW**

Die Zugangsmöglichkeit der IVW wird durch die originäre Tätigkeit, nämlich die Prüfung der Messung der teilnehmenden Webseiten, limitiert. Hierzu steht eine Prüfschnittstelle zur Verfügung. Die Verbindungen sind hierbei verschlüsselt.

bb. **agof**

INFOnline stellt bei besonderer Beauftragung und Weisung des betroffenen Auftraggebers über eine Web-Schnittstelle Daten für agof bzw. deren Partner zur Auswertung bereit. Hierbei erfolgt kein direkter Zugriff auf die Bewegungsdaten der Clients, sondern ausschließlich auf Auszüge (Reports) dieser Daten, welche durch INFOnline erstellt wurden. Die Übertragung der Daten erfolgt verschlüsselt.

cc. **Kunden von INFOnline**

Den Kunden von INFOnline wird über ein HTTPS-Interface ein Zugang zu den eigenen, aggregierten Reports gewährt, die aus den erhobenen Daten des Zählverfahrens durch bereitgestellte Werkzeuge gebildet werden können.

3.2.2.2. Rechenzentrum Düsseldorf

a. **Netzwerk/Applikation**

Der Zugriff auf die Server in Düsseldorf ist nur über eine IP-Sec-Verbindung zwischen den Rechenzentren Bonn und Düsseldorf möglich.

b. **Passwortverfahren**

Das Passwortverfahren für externe Zugriffe auf die im Rechenzentrum betriebenen Maschinen entspricht den Vorgaben in der unternehmenseigenen Passwortrichtlinie für die Hauptverwaltung.

c. **Zugang von außen**

Zugriffe von Kooperationspartnern wie der IVW und agof sind zum RZDUS nicht vorgesehen.

3.2.3. Netzwerksicherheit

Neben dem Verhindern des Zutritts Unbefugter zu den Datenverarbeitungsräumen in den Rechenzentren gehört bei INFOnline zu einem wirksamen Schutz der dort betriebenen

Datenträger auch die Abwehr eines unberechtigten Authentifizierungsversuchs aus dem Internet in das eigene interne Netzwerk im Rechenzentrum. Derartige Zugriffe sind im Gegensatz zu den Räumlichkeiten von INFOnline auf das interne Netzwerk im Rechenzentrum vorgesehen. Durch den Einsatz von Firewalls und Intrusion-Prevention-Systeme sorgt INFOnline dafür, dass die restriktiven Vorgaben hinsichtlich der Zugriffsgewährung von außen wirksam durchgesetzt werden. Die eingesetzten Komponenten werden von den Systemspezialisten regelmäßig gewartet. Zusätzlich sind für die Administratoren abgewiesene Anmeldeversuche anhand erstellter Sicherheitsprotokolle jederzeit nachvollziehbar.

3.2.4. Verfügbarkeitskontrolle

3.2.4.1. Bauliche Sicherheitsinstallationen der Rechenzentren

Rechenzentrum Bonn (Hauptrechenzentrum)

- unterbrechungsfreie Stromversorgung (USV + Dieselaggregat)
- Klimatisierung
- Brandmeldeanlage mit Aufschaltung zur Feuerwehr
- Löschanlage
- Einbruchmeldeanlage mit Aufschaltung zum Sicherheitsdienst
- Zutrittskontrolle durch pers. Chipkarte
- Videoüberwachung
- ZKA-Zulassung
  Das Rechenzentrum genügt den „Sicherheitsanforderungen der deutschen Kreditwirtschaft für das Zahlungssystem electronic cash“.

Rechenzentrum Düsseldorf

- unterbrechungsfreie Stromversorgung (USV + Dieselaggregat)
- Klimatisierung
- Brandmeldeanlage
- Löschanlage
- Einbruchmeldeanlage
- Zutrittskontrolle durch Personal vor Ort
- Videoüberwachung
- Zertifizierungen: ISO27001, BS25999, Payment Card Industry Data Security Standard (PCI-DSS)

3.2.4.2. Software Sicherheitsinstallationen

INFOnline setzt für die gesamte Netzwerk-Infrastruktur Monitoringsysteme ein, die zu jeder Zeit über die Verfügbarkeit der eingesetzten Systeme Auskunft geben können.

Ausfälle von Netzwerkkomponenten, Servern oder Diensten werden 24/7 per Email und automatisiertem Telefonanruf an den Bereitschaftsdienst der INFOnline gemeldet.

3.2.4.3. Datensicherungskonzept

Ein Datensicherungsplan legt fest, welche Daten/Systeme in welchen Abständen und zu welchem Zeitpunkt auf welche Medien bzw. anderen Systeme gesichert werden und wie die Verantwortlichkeiten hierfür geregelt sind. Die Datensicherungsintervalle sind wie folgt ausgestaltet:

Die eingesetzte softwareseitige Backup-Lösung erstellt täglich inkrementelle Datensicherungen hinsichtlich aller eingesetzten Systeme im Rechenzentrum auf entsprechende Sicherungsbänder oder Festplatten.

Darüber hinaus wird eine Vollsicherung der Daten in einem zweiwöchigen Rhythmus durchgeführt. Um eine Wiederherstellbarkeit gem. Art. 32 Abs. 1 lit. d) DSGVO dieser Datensicherungen überprüfen zu können, werden regelmäßig Zufallsdaten wiederhergestellt.

3.2.4.4. Löschung von Daten und Entsorgung von Ausdrucken/Listen

Ausdrucke fallen im Rahmen des Rechenzentrumsbetriebs bei INFOnline nicht an. Sind Datenträger aus den Produktivsystemen für die Löschung vorgesehen, werden diese in den allgemeinen Löschungsprozess der ersten Sicherheitsschicht bei INFOnline mit einbezogen. Der Datenträgertransport aus dem Rechenzentrum erfolgt dabei ausschließlich durch legitimierte Mitarbeiter von INFOnline.

3.2.5. Weitergabe-, Transport-, Übertragungs-, und Datenträgerkontrolle

3.2.5.1. Dateneingang

Im Rahmen der SZMnG-Applikation empfängt INFOnline über das Internet und die im Rechenzentrum eingesetzte Netzwerkinfrastruktur die für das SZMnG-Messverfahren notwendigen Daten.

Der Datenaustausch erfolgt dabei automatisiert durch den Abruf des auf Auftraggeber-seite implementierten SZMnG-Tags.

3.2.5.2. Datenausgang

Als Datenausgang wird bei INFOnline das physische, aktive Versenden von Daten an eine externe Zieladresse verstanden. In diesem Sinne kommt es im Rahmen des Rechenzentrumsbetriebs für das SZMnG lediglich zum Bereitstellen einer Schnittstelle, um Kunden oder angeschlossenen Partnern wie der IVW einen reglementierten Zugriff auf relevante Informationen zu erlauben. Eine Übermittlung von personenbezogenen oder personenbeziehbaren Daten ins Ausland findet nicht statt und ist nicht geplant.

3.2.5.3. Datenträger

Mobile Datenträger kommen im Rechenzentrumsbetrieb nicht zum Einsatz.

Sollte ein Datenträger aussortiert werden, wird dieser in den allgemeinen Datenlöschungs- oder Datenträgervernichtungsprozess bei INFOnline eingebunden.

3.2.6. Protokollierung

Die Protokollierung der Anmeldungen der Mitarbeiter auf ihren Arbeitsplatzsystemen erfolgt in der zweiten Sicherheitsschicht, da der jeweilige aufzeichnende Server ausschließlich im Rechenzentrum betrieben wird. Hierbei wird festgehalten, welcher Mitarbeiter sich zu welcher Zeit am unternehmensinternen Active Directory angemeldet hat. Die Protokollierungsmaßnahmen im SZMnG-Verfahren sind Teil der Ausführungen in der dritten Sicherheitsschicht.

3.2.7. Trennung verschiedener Datenverarbeitungen

Beim Rechenzentrumsbetrieb in der zweiten Sicherheitsschicht ist vor allem die physische Trennung von verschiedenen Datenverarbeitungen relevant. Dies vollzieht sich bei INFOnline durch die Verwendung unterschiedlicher Hardware für unterschiedliche Aufgabenstellungen.

Im Rahmen der weiteren Verarbeitung übernehmen sodann unterschiedliche Maschinen differenzierte Aufgaben (Empfang der Daten, Weiterverarbeitung, Speicherung etc.). Die weitere logische Trennung der Auftraggeber vollzieht sich auf Applikationsebene in der dritten Sicherheitsschicht.

3.3. Dritte Sicherheitsschicht

Die dritte Sicherheitsschicht soll zunächst gewährleisten, dass Personen, die in zulässiger Weise Zugang zu den Datenbeständen haben, nur diejenigen Daten zur Kenntnis bekommen und verarbeiten können, die sie für ihre Aufgabenerledigung benötigen. Dies setzt zwingend voraus, dass vorab festgelegt wird, wer unter welchen Voraussetzungen welche Daten verarbeiten darf. Im Rahmen der Maßnahmendefinition zur technisch-organisatorischen Gewährleistung dieser Vorgaben bedarf es dabei zunächst eines funktionsfähigen Abwehrmechanismus, der eine Datenverarbeitung ohne vordefinierte Rolle wirksam verhindern kann. Gewährt der implementierte Abwehrmechanismus einem Mitarbeiter Zugang und Zugriff zu relevanten Informationen, muss durch ein rollenbasierten Berechtigungskonzept verhindert werden, dass dem Mitarbeiter Zugang zu denjenigen Daten gewährt wird, die für seine konkrete Aufgabenerfüllung nicht notwendig sind.

Darüber hinaus bedeutet die Tatsache, dass jemand grundsätzlich befugt ist, auf bestimmte Datenbestände zuzugreifen, Daten hinzuzufügen, sie zu ändern, zu übermitteln, zu löschen oder sonst zu verwenden, nicht, dass derartige Aktivitäten im Einzelfall auch tatsächlich erforderlich und damit zulässig sind. Daher bedarf es auf Applikationsebene weiterer Maßnahmen, durch die

bewirkt wird, dass die Verantwortung für die einzelnen tatsächlichen Aktivitäten zweifelsfrei festgestellt werden kann.

Die oben dargestellten Prinzipien werden bei INFOnline durch zwei elementare Säulen gestützt. Zum einen werden die (legitimen) Benutzeraktivitäten durch ein bestehendes Berechtigungskonzept bereits vor dem eigentlichen Zugriff auf eventuell personenbezogene Daten kanalisiert, zum andern sorgen entsprechende Kontrollmechanismen dafür, dass Nutzeraktivitäten im Rahmen der Berechtigungen im Nachhinein nachvollziehbar sind.

3.3.1. Berechtigungskonzeptionen im SZMnG-Verfahren

3.3.1.1. Grundsätze

Die Berechtigungsvergabe für Mitarbeiter von INFOnline, die mit der Betreuung des SZMnG-Verfahrens betraut sind, ist in die allgemeine Organisation bei INFOnline eingebettet.
Die Zugangsberechtigung als solche für das SZMnG wird restriktiv gehandhabt. Mitarbeitern wird entsprechend ihrer vorab definierten Rolle auf Basis eines Standard Benutzer-Accounts Zugang zu relevanten Servern gewährt. Vollzugriff erhalten nur Mitglieder der IT-Abteilung als System- und Datenbankadministratoren. Diese Zugriffe werden personenbezogenen bei INFOnline protokolliert.

3.3.1.2. Berechtigungskonzept SZMnG-Logfiles

INFOnline speichert die im Rahmen der Messung anfallenden Logfiles für einen begrenzten Zeitraum von maximal 60 Tagen. IP-Adressen der Internetnutzer werden jedoch vor jeglicher Verarbeitung gekürzt – die Logfiles enthalten somit keine vollständigen IP-Adressen. Logfiles mit Online-Identifiern werden maximal 6 Monate vorgehalten.

a. **INFOnline**

Im Falle einer erforderlichen technischen Überprüfung der Messung kann INFOnline auf die Logfiles der Messung zugreifen. Zugriff auf die Logfiles hat bei INFOnline nur ein eingeschränkter Personenkreis (Mitarbeiter aus dem Bereich Support und Administratoren).

b. **IVW**

Die für den Zugriff legitimierten Mitarbeiter der IVW greifen auf Weisung ihrer Mitglieder, die gleichzeitig Kunden von INFOnline sind, zum einen im Rahmen der Aufnahmeprüfung neuer Angebote, zum anderen bei turnusmäßigen Prüfungen auf ein Audit-System der INFOnline zu. Im Audit-System werden die im Rahmen der Prüfung selbst ausgelösten Zählimpulse ausgewertet. Die Satzung der IVW sieht dabei eine turnusmäßige Überprüfung der Angebote vor. Daneben bestehen anlassbezogene Prüfungen der IVW für den Fall, dass von Dritten Hinweise auf Richtlinienverstöße durch Angebotsportale erbracht werden oder der Kunde selbst den Zählvorgang einer externen Kontrolle unterziehen lassen möchte.

Die Anmeldung der für den Zugriff berechtigten Mitarbeiter der IVW wird auf Seiten von INFOnline protokolliert.

c. **Kunden**

Kunden, die den Service der „Logfilebereitstellung“ nutzen, erhalten über eine Schnittstelle Zugriff auf von INFOnline bereitgestellte Protokolldateien der Messung der jeweiligen Angebote des Kunden (Logstrom).

Für die Bereitstellung des Services „Logfilebereitstellung“ durch INFOnline ist eine besondere Beauftragung durch den Kunden erforderlich.

3.3.2. Protokollierung

Authentifizierungsvorgänge der mit der Wartung des SZMnG betrauten Mitarbeiter von INFOnline werden durch Systemprotokolle erfasst und in entsprechenden Dateien gespeichert.

Diese Protokolldateien werden durch einen Mitarbeiter in regelmäßigen Abständen kontrolliert. Entsprechend den datenschutzrechtlichen Anforderungen an die Eingabekontrolle und der gleichzeitig auszuschließenden Leistungs- und Verhaltenskontrolle der an der Datenverarbeitung beteiligten Person müssen Protokolldaten mit Personenbezug zweckgebunden, vollständig und gleichzeitig datensparsam sein. Der Personenbezug der Protokolldateien resultiert bei INFOnline vor allem aus der Tatsache, dass die Benutzer-Accounts personalisiert sind, um eine Handlung einem Mitarbeiter auch eindeutig zuordnen zu können. Dem Gebot der Vollständigkeit wird dadurch Genüge getan, dass die beteiligten Anwendungen, Maschinen und Personen mit Zeitbezug dokumentiert werden.

Inhaltlich differenzieren die Protokolldateien nach der Schutzbedürftigkeit der personenbezogenen Daten sowie der Eigenschaft des handelnden Mitarbeiters als „regulärer“ Benutzer oder als Administrator. Den Grundsatz bei der Art der Protokollierung bildet dabei die Kernfrage, wer wann mit welchen Mitteln was veranlasst bzw. worauf zugegriffen hat.

Aufgrund der Tatsache, dass Administratoren einen besonderen Einfluss auf die Strukturen eines IT-Systems ausüben können, führt die Nutzung administrativer Rechte bei der INFOnline immer zu einem Eintrag in einer Protokolldatei. Unter der Ausübung einer administrativen Tätigkeit versteht INFOnline Maßnahmen zur Installation, Modifikation und Konfiguration von Software.

Die Protokollauswertung erfolgt dabei nicht auf den Produktivsystemen selbst, sondern auf gesondert ausgewiesenen Protokollservern. Die dort zentral gespeicherten Protokolldateien unterliegen zudem restriktiven Zugriffsbeschränkungen.

3.3.3. Trennung verschiedener Datenverarbeitungen

Die im SZMnG vorgehaltenen Informationen der Auftraggeber sind durch eindeutige Angebotskennungen voneinander getrennt. Zusätzlich besteht zu jeder Angebotskennung eine so genannte „Localliste“. Diese bei INFOnline geführte Liste enthält die URLs der für die Zählung vorgesehenen Digital-Angebote der Auftraggeber sowie der Angebotskennung. Möchte ein

Auftraggeber sein neues Digital-Angebot messen lassen, muss er dies mit einer eindeutigen und gültigen Internet-Adresse bei INFOnline anmelden.

4. Projektspezifische Angaben

a. **Geschäftszwecke/Projektbeschreibung**
Das Skalierbare Zentrale Messverfahren ist ein spezielles Verfahren, das die Requests eines Angebotes (Website/Applikation) in Echtzeit registriert und zählt. Die gemessenen Daten werden auf Systemen von INFOnline gespeichert und analysiert.

b. **Betroffene Personengruppen und Datenarten bzw. –kategorien** • Besucher der Angebotsseiten, Mitarbeiter, Kunden, Kooperationspartner • Technische Protokolldaten der Angebotsbesucher, div. Personalstammdaten von Mitarbeitern, Kunden, Ansprechpartner der Kunden und Kooperationspartner (Kontaktdaten), Auftragsdaten (v.a. Logstrom-Inhalte)	
aa. **Beschreibung der betroffenen Personengruppen**	bb. **Beschreibung der diesbezüglichen Datenarten oder Datenkategorien**
• Websitebesucher	• Technische Protokolldaten IP-Adressen werden vor jeglicher Verarbeitung gekürzt (IPv4: Kürzung um 1 Byte). • Eindeutige Browser- und Geräte-Identifier, sofern vorhanden: ○ Cookie-Kennungen (First-Party und/oder Third-Party Cookie) ○ Signatur bestehend aus der gekürzten Client-IP bzw. X-Forwarded-For (XFF) und dem Useragent (als Hash) ○ AdvertisingIdentifier (ausschließlich als Hash) ○ VendorIdentifier (ausschließlich als Hash) ○ InstallationID (ausschließlich als Hash) ○ AndroidID (ausschließlich als Hash)

• Mitarbeiter von INFOnline	• Stammdaten • Anmeldedaten (Benutzerkennung, Passwort) • Kontaktdaten
• Kunden	• Stammdaten • Auftragsdaten • Kontaktdaten • Stamm- und Kontaktdaten der Ansprechpartner • Dokumentendaten • Abrechnungsdaten • Stamm- und Kontaktdaten der Nutzer • Anmeldedaten (Benutzerkennung, Passwort)
• Kooperationspartner	• Stammdaten • Kontaktdaten • Stamm- und Kontaktdaten der Ansprechpartner der Kooperationspartner • Stamm-, Kontakt- und Anmeldedaten der für das SZMnG-Verfahren bestimmten Mitarbeiter der Kooperationspartner

c. **Empfänger oder Kategorien von Empfängern, denen Daten (regelmäßig) mitgeteilt werden (können)**

- Kunden
- IVW als Kooperationspartner auf Weisung der Auftraggeber
- agof bei gesonderter Beauftragung
- AGMA auf Weisung der Auftraggeber

d. **Löschung der Daten (Regelfristen und Art der Löschung)**

- IP-Adressen werden nur gekürzt für einen begrenzten Zeitraum (maximal 60 Tage) gespeichert. Eine Speicherung vollständiger IP-Adressen findet nicht statt.
- Die Löschung der Bewegungsdaten der Internetnutzer, welche die Kennung/ID bzw. die Signatur eines Clients enthalten, werden nach spätestens 6 Monaten gelöscht.

e.	**Geplante Datenübermittlung an Drittstaaten**				
aa.	**Name des Drittstaates**	bb.	**Empfänger/Kategorien von Empfängern**	cc.	**Art der Daten/Daten-kategorien**
	Keine				

f.	**Zugriffsberechtigte Personengruppen**
	▪ Mitarbeiter von INFOnline ▪ Kunden

5. Dokumenthistorie

Version	Autor	Bemerkung	Datum
Initial	DMC Datenschutz Management & Consulting GmbH & Co. KG	Initial	06/2010
1.0	DSB / INFOnline GmbH	Aktualisierung & Freigabe	03/2011
1.1	DSB / INFOnline GmbH	Aktualisierung	12/2011
2.0	DSB / INFOnline GmbH	Aktualisierung neues SZM	12/2012
2.1	DSB / INFOnline GmbH	Aktualisierung Daten-lieferungen (neues SZMNG)	04/2013
2.2	DSB / INFOnline GmbH	Aktualisierung, Informationen zum bisherigen SZM-System entfernt	10/2014
2.3	DSB / INFOnline GmbH	Ergänzung in Kapitel 4c	12/2014
2.4	DSB / INFOnline GmbH	Anpassung an neues Firmen-CD, kleine Anpassungen	10/2016
2.5	DSB, MZN / INFOnline GmbH	Vollständige Aktualisierung im Hinblick auf DSGVO	03/2018
2.5	JMN/ INFOnline GmbH	Aktualisierung Angaben zum Datenschutzbeauftragten	03/2019