# Die Berichtspflichten des § 5 Absatz 8 Satz 1 Nr. 3 bis 9 des Sächsischen Informationssicherheitsgesetzes

Die Informationssicherheit, d.h. die Vertraulichkeit, Verfügbarkeit und Integrität der mithilfe der Informationstechnik verarbeiteten Daten, ist eine Grundbedingung der digitalen öffentlichen Verwaltung. Gefahren für die Informationssicherheit drohen insbesondere durch Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitung, § 12 Absatz 1 Satz 1 SächsISichG. Die Rechtsgrundlagen aus §§ 12, 13 SächsISichG ermöglichen den staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen den Einsatz von Angriffserkennungssystemen (z.B. Intrusion detection systems [IDS], Security information an event management-Systeme [SIEM-System]), um mögliche Angriffe über die Gesamtheit der IT-Infrastruktur erkennen und analysieren und um hieraus Entscheidungsgrundlagen für die zu treffenden Abwehrmaßnahmen ableiten zu können. Gemeinsam ist diesen Systemen, dass sie nicht stichprobenhaft arbeiten, sondern gesamte Datenströme in Echtzeit auswerten und damit auch große Mengen grundrechtsgeschützter Daten verarbeiten. Die Befugnisse nach §§ 12, 13 SächsISichG unterliegen wegen der damit verbundenen Grundrechtseingriffe strengen Voraussetzungen, deren Einhaltung mit erheblichem technischen und vor allem auch organisatorischem Aufwand für eine staatliche und nicht-staatliche Stelle verbunden ist, die solche IT-Systeme einsetzt.

Zur Transparenz der Wahrnehmung der oben genannten Befugnisse sind Berichtspflichten gegenüber dem Parlament vorgesehen. Das SächsISichG sieht daher in § 5 Absatz 8 vor, in welchem Umfang von den Befugnissen aus Anlass welcher Art von Verdachtslagen Gebrauch gemacht wurde und inwieweit die Betroffenen hierüber benachrichtigt wurden.

Im Einzelnen:

**§ 5 Absatz 8 Satz 1 Nr. 3 SächsISichG**
**„die zur Abwehr von Gefahren für die informationstechnischen Systeme ergriffenen Maßnahmen gemäß § 12“**

Sofern die staatliche oder nicht-staatliche Stelle Angriffserkennungssysteme im o. g. Sinne einsetzt, um mögliche Angriffe über die Gesamtheit der IT-Infrastruktur zu erkennen und zu analysieren, sind diese allgemein zu benennen. Reine Virenscanner oder Spamfilter fallen nicht darunter. Erfolgt hier eine Angabe, so sind zu den weiteren Nummern 4 bis 9 des § 5 Absatz 8 SächsISichG Angaben zu machen.

**§ 5 Absatz 8 Satz 1 Nr. 4 SächsISichG**
**„die Anzahl von Fällen der nicht automatisierten Auswertung, der personenbezogenen Verarbeitung und der Wiederherstellung des Personenbezugs pseudonymisierter Daten bei Protokolldaten gemäß § 13 Absatz 2“**

§ 13 Absatz 2 SächsISichG lässt eine anlassbezogene automatisierte Auswertung für Protokolldaten zu. Anlassbezogen heißt, es existieren tatsächliche Anhaltspunkte für den Fall der Bestätigung eines Gefahrenverdachts durch Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitung. Ausgewertet werden darf in diesem Fall nur automatisiert, d.h. personenbezogene Daten werden auf dieser Stufe nicht von Menschen wahrgenommen. Die automatisierten Analysedurchläufe werden aber manuell ausgelöst. Nur Ausnahmefälle, bei denen eine nicht automatisierte Auswertung, eine personenbezogene Verarbeitung oder die

Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich wurde, sind danach anzugeben.

**§ 5 Absatz 8 Satz 1 Nr. 5 SächsISichG**
**„die Anzahl von Fällen der Speicherung und der Auswertung von Inhaltsdaten und Wiederherstellung des Personenbezugs pseudonymisierter Daten gemäß § 13 Absatz 3“**

§ 13 Absatz 3 SächsISichG lässt ebenso eine anlassbezogene automatisierte Auswertung, allerdings für Inhaltsdaten, zu. Inhaltsdaten sind Daten, die den Inhalt einer Kommunikation betreffen, § 3 Absatz 8 SächsISichG. Anlassbezogen heißt hier, es existieren tatsächliche Anhaltspunkte für den Fall der Bestätigung eines Gefahrenverdachts durch Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitung. Die Speicherung der Inhaltsdaten muss auch weiterhin zum Schutz der technischen Systeme unerlässlich sein. Da Inhaltsdaten dem Fernmeldegeheimnis unterfallen, ist die Anzahl von Fällen der Speicherung und der Auswertung von Inhaltsdaten und Wiederherstellung des Personenbezugs pseudonymisierter Daten anzugeben. Da für diese Maßnahmen eine Anordnungskompetenz durch den Leiter der staatlichen oder nicht-staatlichen Stelle und einem Bediensteten mit Befähigung zum Richteramt vorgesehen ist, sind die Fallzahlen zu protokollieren.

**§ 5 Absatz 8 Satz 1 Nr. 6 SächsISichG**
**„die Anzahl von Fällen der nicht automatisierten Verarbeitung von Daten gemäß § 13 Absatz 4“**

§ 13 Absatz 4 SächsISichG erlaubt die manuelle Auswertung von „Treffern“ der automatisierten Auswertungen, sofern hinreichende tatsächliche Anhaltspunkte für Gefahren für die informationstechnischen Systeme etwa durch Schadprogramme, programmtechnische Sicherheitslücken oder unbefugte Datenverarbeitung enthalten oder Hinweise auf solche Gefahren geben können. Da diese Maßnahmen durch den Leiter der staatlichen oder nicht-staatlichen Stelle und einem Bediensteten mit Befähigung zum Richteramt angeordnet werden müssen, sind die anzugebenden Fallzahlen zu protokollieren.

**§ 5 Absatz 8 Satz 1 Nr. 7 SächsISichG**
**„die Anzahl der durchgeführten, unterbliebenen sowie nachgeholten Benachrichtigungen gemäß § 13 Absatz 5“**

Zur Gewährleistung subjektiven Rechtsschutzes ist die staatliche und nicht-staatliche Stelle bei Maßnahmen nach § 13 Absatz 4 SächsISichG zur Benachrichtigung der betroffenen Person verpflichtet, § 13 Absatz 5 SächsISichG. Diese Pflicht besteht jedoch nicht, wenn dazu in unverhältnismäßiger Weise weitere personenbezogene Daten erhoben werden müssten, § 13 Absatz 5 Satz 1 SächsISichG. Das gilt z.B. für Erfassung von IP-Adressen ohne weitere Folgen für die betroffene Person. Die Benachrichtigungspflicht würde weitere den Grundrechtseingriff vertiefende Ermittlungen erfordern, um die IP-Adresse einer Person zuordnen zu können. Daher besteht hierfür keine Benachrichtigungspflicht.

Die Anzahl der durchgeführten, unterbliebenen sowie nachgeholten Benachrichtigungen sind wegen der verfassungsrechtlich gebotenen aufsichtlichen Kontrolle zu dokumentieren.

**§ 5 Absatz 8 Satz 1 Nr. 8 SächsISichG**
**„die Anzahl von Fällen der Übermittlung von Daten gemäß § 13 Absatz 6 und 7“**

Die Absätze 6 und 7 beziehen sich auf die Übermittlung von Daten an Strafverfolgungsbehörden bzw. bei Absatz 7 auch an das Landesamt für Verfassungsschutz.

Absatz 6 gestattet dabei die Übermittlung von Daten bei Verdachtsfällen von Straftaten nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches und betrifft die bei einer Strafanzeige übermittelten Daten.

Absatz 7 betrifft Zufallsfunde, die einen konkreten Ermittlungsansatz ergeben. Wegen der nachteiligen Folgemaßnahmen für die betroffene Person unterliegt die Regelung in besonderer Weise dem Grundsatz der Verhältnismäßigkeit. Nicht in sämtlichen Fällen dürfen bzw. sollen Daten übermittelt werden. So wird für eine Übermittlung für Zwecke der Strafverfolgung auf die Katalogstraftaten gemäß § 100a der Strafprozessordnung abgestellt, die eine Telekommunikationsüberwachung rechtfertigen würden.

Die Anzahl dieser Datenübermittlungen ist anzugeben.

**§ 5 Absatz 8 Satz 1 Nr. 9 SächsISichG**
**„den Umgang mit unzulässig erlangten Daten, die den Kernbereich privater Lebensgestaltung betreffen, gemäß § 13 Absatz 8“**

§ 13 Absatz 8 SächsISichG dient dem Schutz besonders sensibler Daten. Daten aus dem Kernbereich privater Lebensgestaltung sind geeignet die betroffene Person in ihrer beruflichen oder gesellschaftlichen Stellung zu beeinträchtigen. Daher dürfen sie nicht gespeichert oder verwendet werde. Sie sind unverzüglich zu löschen. Ihre Auswertung und Löschung muss dokumentiert werden, § 13 Absatz 8 Satz 5 SächsISichG. Die Anzahl der dokumentierten Fälle ist in § 5 Absatz 8 Satz 1 Nr. 9 SächsISichG anzugeben.