Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (Sächsisches Datenschutzgesetz – SächsDSG)
http://www.revosax.sachsen.de/Details.do?sid=1489112710514

§ 9 **Maßnahmen zur Gewährleistung des Datenschutzes**

(1) **Öffentliche Stellen, die personenbezogene Daten verarbeiten, haben alle angemessenen personellen, technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Datenverarbeitung zu gewährleisten. Die Grundsätze der Datenvermeidung und Datensparsamkeit sind zu beachten.**

(2) Werden personenbezogene Daten verarbeitet, sind nach dem jeweiligen Stand der Technik Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass
1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

(3) Die Staatsregierung wird ermächtigt, durch **Rechtsverordnung** die in den Absätzen 1 und 2 genannten Anforderungen und Maßnahmen nach dem jeweiligen Stand der Technik näher zu bestimmen und fortzuschreiben.

(4) Werden personenbezogene Daten in Akten verarbeitet, sind besondere Maßnahmen zu treffen, um zu verhindern, dass Unbefugte bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung auf die Daten zugreifen können.

Fundstelle 1:
http://www.datenschutz.hessen.de/tb39k05.htm
[39. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten Professor Dr. Michael Ronellenfitsch]

5.1.1.2 Automatische Weiterleitung an externe Mail-Adressen

Bei meinen Prüfungen musste ich feststellen, dass in einigen wenigen Fällen Mitarbeiter für ihr dienstliches, persönliches Postfach eine automatische Weiterleitung an ein privates Postfach eingerichtet hatten. Teilweise war es der Wunsch, von zu Hause weiterarbeiten zu können. In anderen Fällen war es jedoch der Wunsch, immer auf dem Laufenden zu sein. Durch die Verbreitung von Mobilfunkgeräten, die auch die Möglichkeit haben, eine Verbindung zum Internet herzustellen oder E-Mails zu empfangen, zeigte sich eine neue Qualität. So hatte ein Bürgermeister mit einem Mobilfunkbetreiber einen Vertrag zu einem Smartphone vom Typ Blackberry geschlossen. Vertragsbestandteil war die Möglichkeit, e-Mails zu empfangen. In dem Wunsch, jederzeit über eingehende E-Mails informiert zu sein, hatte er die automatische Weiterleitung der an ihn gerichteten E-Mails vom Mail-Server der Kommune einrichten lassen.

Die **externe Weiterleitung ist problematisch**, da **der interne Absender nicht davon ausgehen kann, dass seine E-Mail das Verwaltungsnetz verlässt und auf dem Mailserver eines privaten Betreibers gespeichert wird.** Ebenso wenig muss dies ein Absender einer anderen Behörde erwarten, der über einen gemeinsamen Dienstleister mit der Kommune E-Mails austauscht. Auch ein Bürger darf davon ausgehen, dass seine E-Mail nicht noch bei einem weiteren privaten Betreiber gespeichert wird.

[…]

Solange kein ausreichender Datenschutz gewährleistet wird, ist auf eine automatische Weiterleitung an externe Postfächer zu verzichten. Als eine Maßnahme sollte die technische Möglichkeit deaktiviert werden, die es Benutzern erlaubt automatische Weiterleitungen an externe Postfächer einzurichten.

Fundstelle 2:
http://www.saechsdsb.de/informationen-oeb/arbeitshilfen-oeb
Musterdienstvereinbarung über die Nutzung elektronischer Kommunikationssysteme (E-Mail)

2 Grundsätze
[…]
(3) Der Nutzer ist für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich.
[…]
(4) Die elektronische Kommunikation ist vorrangig einzusetzen, wenn sie für die Übermittlung geeignet und wirtschaftlich ist und keine rechtlichen Gründe entgegenstehen. **Aus Gründen des Datenschutzes und des Geheimschutzes ist die elektronische Kommunikation nur für Nachrichten zulässig, die keine schützenswerten Daten enthalten** (vgl. Nr. 33 Abs. 1 SächsDienstO). Auf die Beachtung der Aussagen und Festlegungen zu Sicherheit und Datenschutz (siehe Punkt 5) wird ausdrücklich verwiesen. […]

5 Sicherheit und Datenschutz
(1) **Die Kommunikation über das Internet ist mit erheblichen Gefährdungen des Datenschutzes und der Datensicherheit verbunden**. So ist es nicht transparent, welchen Übertragungsweg die Daten nehmen oder über welche Vermittlungsrechner die Daten übertragen werden. Eine gezielte Manipulation oder unbefugte Verwendung von Informationen kann somit nicht ausgeschlossen werden. Deshalb wurden Sicherheitsmaßnahmen, wie z. B. Protokollierungen des Internetverkehrs, Schutz vor Fremdbenutzung und ein zentrales Virenscanning in das Internet-Zugangssystem integriert. Sämtliche Sicherheitseinstellungen dürfen nicht durch den Nutzer verändert oder deaktiviert werden. Darüber hinaus ist es erforderlich, dass jeder Nutzer sorgfältig die in dieser Dienstvereinbarung beschriebenen Sicherheitsmaßnahmen befolgt und die Bestimmungen des Daten- und Geheimschutzes einhält.
[…]
(5) **Beim Versand von elektronischer Post sind Sicherheit und Datenschutz zu gewährleisten**. Wer den elektronischen Versand von Schriftstücken anordnet oder nach eigenem Ermessen selbst vornimmt, trägt die Verantwortung für die Entscheidung, dass die Risiken vertretbar sind.
(6) Der Einsatz der elektronischen Post ohne zusätzliche Sicherheitsvorkehrungen (z. B. elektronische Signatur oder elektronische Verschlüsselung) ist nur für Nachrichten zulässig, die keine personenbezogenen Daten oder sonstigen schützenswerten Informationen enthalten oder die nicht der Schriftform bedürfen. […]

Ebenda: **Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz**