

## A N T W O R T

zu der

Anfrage des Abgeordneten Andreas Augustin (PIRATEN)

betr.: Entsorgung elektronischer und magnetischer Speichermedien der Landesministerien inklusive Staatskanzlei sowie der saarländischen Behörden

Elektronische und magnetische Speichermedien haben in den letzten Jahrzehnten eine immer wichtigere und elementarere Rolle bei der täglichen Büroarbeit eingenommen und es gibt heutzutage praktisch keinen Arbeitsplatz mehr, der ohne Computer oder Laptop auskommt. In saarländischen Ministerien und Behörden wird in einem besonderem Maße mit vertraulichen persönlichen Daten gearbeitet.

Sowohl elektronische als auch magnetische Speichermedien stellen allerdings in Hinsicht auf den Datenschutz besondere Anforderungen an deren Entsorgung. Achtlos entsorgte Festplatten enthalten noch alle Daten, die im Laufe ihrer Einsatzzeit auf ihnen gespeichert wurden. Selbst einfach formatierte Datenträger, die einen leeren Eindruck erwecken, können mit sehr wenig Aufwand und frei zugänglichen Programmen zu weiten Teilen wiederhergestellt werden. Selbst wenn Festplatten mehrfach mit Zufallsdaten überschrieben werden, können unter verstärktem Aufwand noch Informationen aus diesen rekonstruiert werden. Auch während des Betriebs ausgefallene und defekte Datenträger, die von einem PC nicht mehr erkannt werden, können oft fast vollständig wiederhergestellt werden.

Eine ausreichende Sicherheit wird bei elektronischen und magnetischen Speichermedien, ähnlich wie bei herkömmlichen Papierakten, nur durch eine fachgerechte physische Vernichtung erreicht.

Neben den meist stationär in den Ministerien bzw. Behörden eingesetzten Speichermedien, wie z.B. Computerfestplatten, die vor Diebstahl oder Verlust in der Regel ausreichend geschützt sind, werden in den letzten Jahren verstärkt mobile elektronische Speichermedien wie USB-Sticks, Speicherkarten oder Smartphones eingesetzt. Bei diesen besteht während ihrer Lebensdauer auf Grund ihrer Größe und Mobilität ein erhöhtes Verlust- und Diebstahlrisiko, wodurch alle auf ihnen gespeicherten Daten in unbefugte Hände fallen könnten. Dieses Risiko kann in der Regel nur entweder durch ein komplettes Einsatzverbot, welches jedoch nicht immer praktikabel erscheint, oder durch eine ausreichende Verschlüsselung des Datenträgers vermieden werden. Bei Smartphones gibt es darüber hinaus noch die Möglichkeit, per Fernwartung eine Datenlöschung zu veranlassen, die zumindest die Wiederherstellung erschweren würde.

Wie werden elektronische und magnetische Speichermedien der Landesministerien, der Staatskanzlei und soweit bekannt der weiteren saarländischen Behörden entsorgt? Für den Fall, dass es keine einheitlichen Richtlinien gibt, wird um genaue Aufschlüsselung der jeweiligen Richtlinien der verschiedenen Behörden gebeten.

Zu Frage 1:

Die Entsorgung elektronischer und magnetischer Speichermedien ist zentral in folgenden Richtlinien geregelt:

- Richtlinien für die Vergabe von Aufträgen über Lieferungen und Leistungen durch die saarländische Landesverwaltung (Beschaffungsrichtlinien) vom 16. September 2008 (Amtsbl. S. 1681), geändert durch Änderung der Richtlinien für die Vergabe von Aufträgen über Lieferungen und Leistungen durch die saarländische Landesverwaltung vom 28. Dezember 2010 (Amtsbl. II 2011 S. 3):

Tz. 19 „Entsorgung von IuK-Komponenten“:

Hier ist festgelegt, dass die zu entsorgenden IuK-Komponenten dem Landesamt für Zentrale Dienste – Zentrale Datenverarbeitungsstelle für das Saarland (ZDV-Saar) zu übergeben sind. Die Entsorgung hat unter Gewährleistung der Datensicherheit und des Datenschutzes sowie unter Beachtung von Umweltauflagen zu erfolgen. Die organisatorischen Einzelheiten sind in den „Richtlinien für die Beschaffung von Lieferungen und Leistungen auf dem Gebiet der Informations- und Kommunikationstechnologie (IuK-BER) geregelt.

- Richtlinien für die Beschaffung von Lieferungen und Leistungen auf dem Gebiet der Informations- und Kommunikationstechnik (IuK-BER) vom 1. Mai 2010 (Amtsbl. II S. 306), geändert durch Erlass vom 30. August 2011 (Amtsbl. II S. 1002)

- Tz. 3 „Verwertung, Entsorgung ausgesonderter IuK-Komponenten“

Hier ist die Übergabe der IuK-Komponenten an die ZDV-Saar geregelt. Diese prüft, ob die Komponenten weiter verwendet werden können. Bei defekten IuK-Komponenten sind die Festspeicher auszubauen und einer BSI\*-konformen Entsorgung zuzuführen (\*BSI – Bundesamt für Sicherheit in der Informationstechnik). Die übrigen Bauteile sind – unter Beachtung der erforderlichen Datenschutz- und Umweltauflagen – zu entsorgen.

In der Praxis sieht dies beim zentralen IT-Dienstleister, der ZDV-Saar, so aus, dass für alle beschafften Server, PCs und Laptops ein Festplattenverwurf ausgeschrieben ist. Dies bedeutet, dass defekte Festplatten immer beim Bedarfsträger verbleiben und bei einem Austausch auf keinen Fall die ZDV-Saar verlassen. Die zu entsorgenden Datenspeicher werden beim Landesamt für Zentrale Dienste (LZD) in einem verschlossenen Raum/Behälter gesammelt. Zu entsorgende Datenspeicher/Festplatten werden dokumentiert (Kopie Label auf Festplatte – Seriennummer) und der Entsorgungsfirma zum Schreddern nach BSI-Richtlinien übergeben. Die Firma dokumentiert die ordnungsgemäße Entsorgung nach den Richtlinien des BSI.

Neben den o.a. Richtlinien ist in der „Gemeinsamen Geschäftsordnung der obersten Landesbehörden (GGO)“ vom 16.10.2001 in der Anlage 2 die „Nutzung elektronischer Kommunikationssysteme“ geregelt. Hier werden u.a. die möglichen Bedrohungen aufgezeigt. Zudem ist vorgegeben, dass diesen möglichen Bedrohungen mit geeigneten technischen und insbesondere auch organisatorischen Maßnahmen zu entgegnen ist.

Darüber hinaus ist die „Richtlinie für die Planung und Realisierung der Sicherheit der Informationstechnik im Rahmen informationstechnischer und kommunikationstechnischer Verfahren – IT-Sicherheitsrichtlinie – vom 05.06.2003“ bei der Planung und Realisierung der Sicherheit der Informationstechnik im Rahmen informationstechnischer und kommunikationstechnischer Verfahren in der Landesverwaltung anzuwenden. Diese Richtlinie schließt in die zu definierenden und zu erreichenden Sicherheitsziele auch das Abfallgesetz (Entsorgung von Geräten und Material) und somit die ordnungsgemäße und sichere Entsorgung von elektronischen und magnetischen Speichermedien mit ein.

Die Entsorgung elektronischer und magnetischer Speichermedien erfolgt daher grundsätzlich über das Landesamt für Zentrale Dienste (LZD) – Abteilung B, Zentrale Datenverarbeitungsstelle für das Saarland (ZDV-Saar). Bei einigen Ressorts erfolgt die Entsorgung elektronischer Datenträger – insbesondere wenn es sich um größere Chargen handelt oder wenn eigene Vorschriften existieren – auch in eigener Verantwortung:

Ressort	Vorgehen	Vorschriften
CdS	Elektronische und magnetische Speichermedien werden zur Entsorgung an die ZDV-Saar weitergeleitet.	IT-Beschaffungsrichtlinien IuK-BER
MfIS – Ministerium  Vollzugs- polizei	Elektronische und magnetische Speichermedien werden zur Entsorgung an die ZDV-Saar weitergeleitet.  Die Entsorgung erfolgt durch die Dienststelle des LPP 4.4.2 (Endgerätebetreuung/ Inventarisierung). Die Datenträger werden dort in abschließbaren Boxen gesammelt und in regelmäßigen Abständen durch die Fa. Reisswolf in Saarbrücken zur zertifizierten Vernichtung abgeholt. Die Entsorgungszertifikate werden bei LPP 4.4.2 vorgehalten	IT-Beschaffungsrichtlinien IuK-BER  Betriebsregelung über die Vernichtung/Entsorgung von digitalen Datenträgern bei der saarl. Vollzugspolizei vom 01.08.2008“
MFE	Elektronische und magnetische Speichermedien werden zur Entsorgung an die ZDV-Saar weitergeleitet.	IT-Beschaffungsrichtlinien IuK-BER
MfSGFF	Die Speichermedien werden mehrfach gelöscht und zur Entsorgung zur ZDV-Saar verbracht oder direkt zu einem BSI-zertifizierten Entsorger geliefert und dort geschreddert.	IT-Beschaffungsrichtlinien IuK-BER IT-Sicherheitsrichtlinie
MBK	Elektronische und magnetische Speichermedien werden im Bildungsministerium zur Entsorgung an die ZDV-Saar weitergeleitet.	IT-Beschaffungsrichtlinie IuK-BER
MfWAEV	Alle Datenträger werden in einer verschlossenen Tonne der Fa. Reisswolf, die sich in einem verschlossenen Raum befindet, gesammelt. Bei Bedarf wird die Tonne dann von der Firma abgeholt und die Datenträger BSI-konform vernichtet.	IT-Sicherheitsrichtlinie
MfUV	Elektronische und magnetische Speichermedien werden zur Entsorgung an die ZDV-Saar weitergeleitet.	IT-Beschaffungsrichtlinie IuK-BER IT-Sicherheitsrichtlinie
MdJ	Im Geschäftsbereich des Ministeriums der Justiz ist die Entsorgung von Elektronikschrott im Erlassweg geregelt. Danach sind die Justizbehörden gehalten, alle nicht mehr benötigten Datenträger zu sammeln und unserer zentralen EDV-Koordinationsstelle zu übergeben. Alle Datenträger werden sodann gegen Übergabebeleg der ZDV-Saar zur fachgerechten Entsorgung überlassen. Dies ist in der Vergangenheit mit einer einzigen Ausnahme auch so gehandhabt worden. In einem Fall war <u>durch</u>	IT-Beschaffungsrichtlinien IuK-BER  Erlasse MdJ vom 23.06.2006 und 23.05.2012

Ressort	Vorgehen	Vorschriften
	<u>Vermittlung der ZDV-Saar</u> die Firma SEV GmbH zur Abholung großer Mengen Elektronikschrott beauftrag worden. Bei dieser Gelegenheit wurden die Datenträger einer gesonderten Entsorgung zugeführt.	

Seit wann sind die derzeitigen Richtlinien in Kraft?  
 Falls es unterschiedliche Richtlinien geben sollte,  
 bitte nach den jeweiligen Ministerien bzw. Behörden aufschlüsseln.

Zu Frage 2:

Zentrale Richtlinien	Gültig seit
Richtlinien für die Vergabe von Aufträgen über Lieferungen und Leistungen durch die saarländische Landesverwaltung (Beschaffungsrichtlinien)	Die Beschaffungsrichtlinien datieren vom 16.08.2008; die Vorgaben zur Entsorgung von IuK-Komponenten sind in der letzten Änderung vom 28.12.2010 aufgenommen worden. Gültig seit 1. Januar 2011
Richtlinien für die Beschaffung von Lieferungen und Leistungen auf dem Gebiet der Informations- und Kommunikationstechnik (IuK-BER)	Die IuK-BER datieren vom 02.05.2010; die Vorgaben zur Entsorgung von IuK-Komponenten sind in der letzten Änderung vom 30.08.2011 aufgenommen worden. Gültig seit 1. Oktober 2011
„Gemeinsamen Geschäftsordnung der obersten Landesbehörden (GGO)“; hier: Anlage 2 die „Nutzung elektronischer Kommunikationssysteme“	Letzter Stand: 16.10.2001
„Richtlinie für die Planung und Realisierung der Sicherheit der Informationstechnik im Rahmen informationstechnischer und kommunikationstechnischer Verfahren – IT-Sicherheitsrichtlinie –	Letzter Stand: 05.06.2003
Allerdings bietet die ZDV-Saar seit etwa 20 Jahren die zentrale und zertifizierte Entsorgung elektronischer und magnetischer Speichermedien in ihrem Leistungsportfolio an.	

Darüber hinaus gibt es bei den Ressorts noch folgende Richtlinien, die die Entsorgung elektronischer und magnetischer Speichermedien regeln:

<b>Richtlinien/Erlasse der Ressorts</b>		
<b>Ressort</b>	<b>Richtlinien/Erlasse</b>	<b>Gültig seit</b>
CdS	IT-Benutzerordnung	Stand: 16.03.2012
MfIS – Ministerium Vollzugspolizei	Betriebsregelung über die Vernichtung/Entsorgung von digitalen Datenträgern bei der saarl. Vollzugspolizei	Stand: 01.08.2008
MFE	IT-Dienstanweisung für das Ministerium der Finanzen  Dienstanweisung für IT-unterstützte Arbeitsplätze bei den Finanzämtern  IT-Dienstvereinbarung des Landesamtes für Zentrale Dienste	Stand: 01.11.2004  Stand 02.05.2007  Stand: 01.10.2011
MfSGFF	IT-Dienstanweisung (damals Ministerium für Frauen, Arbeit, Gesundheit und Soziales)	Stand: 15.08.2000
MfWAEV	IT-Dienstanweisung (damals Ministerium für Wirtschaft)	Stand: 07/2004
MfUV	IT-Sicherheitsrichtlinie des Umweltministeriums - Ziffer 7.8 Datenträgervernichtung - Ziffer 7.6 Verwaltung und Handhabung von digitalen Datenträgern  Richtlinie „Umgang mit Hard- und Software“ - Ziffer 26 Aussonderung von digitalen Datenträgern - Ziffer 25 Löschen von Daten	Stand: August 2009  Stand: August 2009  Stand: 03.05.2010
MdJ	Erlass zur Entsorgung von Elektroschrott im Geschäftsbereich des Ministeriums der Justiz	Erlass des MdJ

Seit wann gibt es überhaupt irgendwelche, ggf. von den aktuellen Richtlinien abweichende, Richtlinien? Wie wurde vor dem erstmaligen Inkrafttreten entsprechender Richtlinien bezüglich der Entsorgung entsprechender Medien verfahren?

### Zu Frage 3:

Vor dem Inkrafttreten der o.a. Richtlinien gab es bereits Regelungen, die sich auch auf die Vernichtung von Datenträgern bezogen. So gab es für das Innenministerium sowie das Wirtschaftsministerium eine „Richtlinie zur Vernichtung von Schriftgut und sonstigen Datenträgern“ aus dem Jahr 1989 bzw. 1991. Auch in der „Dienstanweisung für den Einsatz von EDV-Verfahren auf Mehrplatzsystemen bei Gerichten und Staatsanwaltschaften im Bereich des Ministeriums der Justiz des Saarlandes“ war die Beachtung der v.g. Richtlinie des Innenministeriums vorgegeben. Auch die unter Tz. 2 aufgeführten ressortspezifischen Regelungen schreiben den Umgang mit Datenträgern vor.

Zudem bietet der zentrale IT-Dienstleister der saarländischen Landesverwaltung, die ZDV-Saar, den Ressorts seit etwa 20 Jahren die zentrale und zertifizierte Entsorgung elektronischer und magnetischer Speichermedien in ihrem Leistungsportfolio an.

Inwieweit sind die geltenden Richtlinien mit dem Unabhängigen Datenschutzzentrum abgestimmt?  
Inwieweit fand eine Überprüfung der Richtlinien und deren Einhaltung durch das Unabhängige Datenschutzzentrum statt?

### Zu Frage 4:

Beim Erlass der GGO vom 16.10.2001 fand eine intensive Abstimmung mit dem saarländischen Datenschutzbeauftragten statt. Dieser war auch an der Ausarbeitung der entsprechenden Gemeinsamen Geschäftsordnung der Anlage 2 GGO intensiv beteiligt. Dies gilt in gleicher Weise für die „Richtlinie für die Planung und Realisierung der Sicherheit der Informationstechnik im Rahmen informationstechnischer und kommunikationstechnischer Verfahren – IT-Sicherheitsrichtlinie –“.

Die Beschaffungsrichtlinie und die IuK-BER wurden nicht mit dem Unabhängigen Datenschutzzentrum abgestimmt.

Eine Überprüfung der Einhaltung der Richtlinien durch die einzelnen Ressorts erfolgte bislang nicht durch das Unabhängige Datenschutzzentrum. Allerdings ist die Frage des Umgangs mit den „Altrechnern“ und zugehörigen Datenträgern sowie die Frage der Verschlüsselung mobiler Endgeräte integraler Bestandteil von Datenschutzprüfungen, die das Unabhängige Datenschutzzentrum in verschiedenen Dienststellen durchgeführt hat und auch weiterhin durchführen wird. Im Rahmen dieser Datenschutzprüfungen werden auch die evtl. Zwischenlagerung der zu entsorgenden Datenträger und die entsprechenden Entsorgungsnachweise in Augenschein genommen. Im Rahmen des Einführungsbesuches der Landesbeauftragten für Datenschutz und Informationsfreiheit, Frau Thieser, bei der ZDV-Saar wurde auch die ordnungsgemäße Entsorgung besprochen.

Inwieweit eine Abstimmung der o.a. ressortspezifischen Regelungen mit dem Unabhängigen Datenschutzzentrum oder dem behördlichen Datenschutzbeauftragten stattfand, ist der nachfolgenden Tabelle zu entnehmen.



<b>Richtlinien/Erlasse der Ressorts</b>			
<b>Ressort</b>	<b>Richtlinien/Erlasse</b>	<b>Abstimmung mit dem Unabhängigen Datenschutzzentrum oder dem behördlichen Datenschutzbeauftragten</b>	<b>Prüfung durch das Unabhängige Datenschutzzentrum oder den behördlichen Datenschutzbeauftragten</b>
CdS	IT-Benutzerordnung	Abstimmung mit dem behördlichen Datenschutzbeauftragten	Eine Überprüfung fand bislang nicht statt.
MfIS – Vollzugspolizei	Betriebsregelung über die Vernichtung/ Entsorgung von digitalen Datenträgern bei der saarl. Vollzugspolizei	Abstimmung mit den behördlichen Datenschutzbeauftragten der damaligen Landespolizeidirektion und des damaligen Landeskriminalamtes	Eine Überprüfung fand bislang nicht statt.
MFE	IT-Dienstanweisung (damals das Ministerium der Finanzen)	Abstimmung mit den behördlichen Datenschutzbeauftragten	Eine Überprüfung fand bislang nicht statt.
MfSGFF	IT-Dienstanweisung (damals Ministerium für Frauen, Arbeit, Gesundheit und Soziales)	Abstimmung mit dem Landesdatenschutzbeauftragten	Eine Überprüfung fand bislang nicht statt.
MfWAEV	IT-Dienstanweisung des damaligen Ministeriums für Wirtschaft	Abstimmung mit dem damaligen Vertreter des Landesdatenschutzbeauftragten, Herrn Simon	Eine Überprüfung fand bislang nicht statt.
MfUV	IT-Sicherheitsrichtlinie des Umweltministeriums - Ziffer 7.8 Datenträgervernichtung - Ziffer 7.6 Verwaltung und Handhabung von digitalen Datenträgern  Richtlinie „Umgang mit Hard- und Software“ - Ziffer 26 Aussonderung von digitalen Datenträgern - Ziffer 25 Löschen von Daten	Abstimmung mit dem Unabhängigen Datenschutz-Zentrum	Eine Überprüfung fand bislang nicht statt.

MdJ	Erlass zur Entsorgung von Elektroschrott im Geschäftsbereich des Ministeriums der Justiz	Keine Abstimmung mit dem Unabhängigen Datenschutzzentrum, da nur ergänzende Regelungen zur GGO bzw. IT-BER	Eine Überprüfung fand bislang nicht statt.
-----	--	--	--

Wird die Einhaltung der entsprechenden Richtlinien überprüft und welche Maßnahmen werden seitens der Landesministerien, Staatskanzlei und Behörden unternommen, um eine vollständige sachgerechte Entsorgung insbesondere von mobilen Speichermedien wie USB-Sticks, externen Festplatten oder Speicherkarten sicherzustellen?

Zu Frage 5:

Sofern die Entsorgung zentral über die ZDV-Saar erfolgt, werden alle getätigten Entsorgungen entsprechend dokumentiert und diese Dokumente aufbewahrt. Zuständig ist hierfür das Sachgebiet B 33 „eGovernment, IT-Support, IT-Sicherheit, IT-Beschaffung“.

Die Handhabung in den Ressorts ist der nachfolgenden Tabelle zu entnehmen.

Ressort	Vorgehen
CdS	Die Mitarbeiterinnen und Mitarbeiter erhalten bei Beginn ihrer Tätigkeit in der Staatskanzlei eine entsprechende IT-Benutzerordnung. Es finden darüber hinaus Informationsveranstaltungen und Schulungen zur Informationsvermittlung und zur Sensibilisierung für die Fragen der IT-Sicherheit statt. Die Gefahren der Rekonstruktion von Daten auf gelöschten Speichermedien ist ausdrücklich Gegenstand der Informations- und Sensibilisierungsveranstaltungen. Im Jahr 2012 fanden insgesamt 4 Veranstaltungen zum Thema IT-Sicherheit in der Staatskanzlei statt.
MfIS – Ministerium	Elektronische und magnetische Speichermedien werden zur Entsorgung an die ZDV-Saar weitergeleitet.
Vollzugs- polizei	Die Entsorgung erfolgt durch die Dienststelle des LPP 4.4.2 (Endgerätebetreuung/ Inventarisierung). Die Datenträger werden dort in abschließbaren Boxen gesammelt und in regelmäßigen Abständen durch die Fa. Reisswolf in Saarbrücken zur zertifizierten Vernichtung abgeholt. Die Entsorgungszertifikate werden bei LPP 4.4.2 vorgehalten
MFE	Die Mitarbeiter werden bei der Übergabe entsprechender Geräte in den Umgang eingewiesen und gleichzeitig auf die IT-Dienstanweisung verwiesen. Diese steht allen Mitarbeitern im Intranet zur Verfügung.
MfSGFF	Die Einhaltung der entsprechenden Richtlinien wurde zuletzt von der KEUF (Kontrollstelle EU-Fonds) durch externe Prüfer überprüft. Mobile Speichermedien werden nur ausnahmsweise ausgegeben. Die Entsorgung erfolgt so wie die Entsorgung der restlichen Speichermedien (siehe hierzu MfSGFF Tz. 1).
MBK	Als mobile Datenträger im Sinne der Frage werden im MBK ausschließlich USB-Sticks eingesetzt. Diese werden zentral verwaltet und bei Bedarf an Mitarbeiter ausgegeben und nach Verwendung wieder zurückgenommen. Die Entsorgung erfolgt so wie die Entsorgung der restlichen Speichermedien (siehe hierzu MBK zu Frage 1).
MfWAEV	Alle Datenträger werden in einer verschlossenen Tonne der Fa. Reisswolf, die sich in einem verschlossenen Raum befindet, gesammelt. Bei Bedarf wird die Tonne dann von der Firma abgeholt und die Datenträger BSI-konform vernichtet.
MfUV	Die Liste der zu entsorgenden Geräte wird vom Haushaltsbeauftragten und Leiter des IT-Referates gegengezeichnet. In der Gerätedatenbank wird ein entsprechender Vermerk angebracht. Die Übergabe der Geräte an die ZDV-Saar oder einen zertifizierten Entsorgungsbetrieb erfolgt über Empfangsbestätigung.
MdJ	Im Geschäftsbereich des Ministeriums der Justiz ist die Entsorgung von Elektronikschrott im Erlassweg geregelt. Danach sind die Justizbehörden gehalten, alle nicht mehr benötigten Datenträger zu sammeln und unserer zentralen EDV-Koordinationsstelle zu übergeben. Alle Datenträger werden sodann gegen Übergabebeleg der ZDV-Saar zur fachgerechten Entsorgung überlassen. In einem Ausnahmefall wurde <u>auf Vermittlung der ZDV-Saar</u> ein zertifizierter Fachbetrieb mit der Abholung großer Mengen Elektronikschrott beauftragt. Bei dieser Gelegenheit wurden die Datenträger einer fachgerechten Entsorgung zugeführt.

Werden bei mobilen elektronischen und magnetischen Speichermedien wie Laptops, Smartphones, USB-Sticks, externen Festplatten oder Speicherkarten bestimmte Sicherheitsvorkehrungen (zum Beispiel Verschlüsselung) unternommen, damit die Daten auch bei Verlust oder Diebstahl ausreichend geschützt werden? Falls ja, welche Methoden werden hierfür eingesetzt und seit wann? Sollte es hier Unterschiede geben, bitte nach Ministerien bzw. Behörden aufschlüsseln.

#### Zu Frage 6:

Zurzeit existiert noch keine einheitliche landesweite Regelung. Teilweise werden Festplatten, USB-Sticks, Speicherkarten und Smartphones verschlüsselt. Hierzu werden unterschiedliche symmetrische oder asymmetrische Verfahren eingesetzt (beispielsweise Bitblocker, TrueCrypt, Blackberry-Infrastruktur).

Die Handhabung in den Ressorts ist der nachfolgenden Tabelle zu entnehmen:

<b>Ressort</b>	<b>Vorgehen</b>
CdS	<p>Die IT-Benutzerordnung der Staatskanzlei verpflichtet dazu, besonders schützenswerte oder vertrauliche Daten zu verschlüsseln sowie sie außerhalb des Landesdatennetzes transportiert werden. Die Thematik ist auch Teil der Informationsveranstaltungen zur IT-Sicherheit.</p> <p>Sensible Daten werden mit PGP verschlüsselt. Seit 2011 wird auf mobilen Endgeräten auch TrueCrypt eingesetzt. Die Installation und Einrichtung der Verschlüsselungssoftware wird durch den Benutzerservice vorgenommen.</p>
MfIS – Ministerium	<p>Mobile elektronische und magnetische Speichermedien in Notebooks, Netbooks, etc. werden mit aktueller Verschlüsselungssoftware geschützt. Derzeit werden hierfür die Software-Produkte SafeGuard, TrueCrypt und Secude Finally Secure eingesetzt. Die Festplattenverschlüsselung wird seit dem Jahre 2009 praktiziert.</p> <p>Bei Smartphones können – je nach Softwarestand – die SD-Karten verschlüsselt werden. Sie sind dann nur mit diesem einen Endgerät nutzbar und die Daten können nur damit ausgelesen werden.</p>
MFE	Bei Laptops stellt das MFE den jeweiligen Bediensteten das Softwareprodukt PGP zur Verschlüsselung zur Verfügung. Mitarbeiter, die sensible Daten auf mobilen Endgeräten speichern, werden durch den Benutzerservice auf die Gefahren bei gleichzeitigem Verweis auf die IT-Dienstanweisung hingewiesen.
MfSGFF	Bei mobilen elektronischen Speichermedien werden sowohl asymmetrische als auch symmetrische Verschlüsselungsverfahren eingesetzt.
MBK	Die Anwender sind gehalten, auf Notebooks keine Daten abzulegen, um keine Angriffsflächen zu bieten. USB-Sticks werden bei besonderem Schutzbedürfnis verschlüsselt.

MfWAEV	Die Festplatten von Notebooks werden (seit ca. 10 Jahren) grundsätzlich verschlüsselt (früher mit SafeGuard, ab Windows 7 mit Bitlocker). Bei Smartphones werden – soweit möglich – Verschlüsselungsfunktionen genutzt. Die „Benutzerrichtlinie für den Umgang mit Smartphones und PAD-PC“ verbietet die Speicherung von Daten auf den Geräten, die nach der IT-Sicherheitsrichtlinie des Saarlandes einen hohen oder sehr hohen Schutzbedarf haben.
MfUV	Im Umweltministerium ist seit 2009 die „allgemeine Sicherheitsrichtlinie Notebook“ in Kraft. Verschlüsselungen werden bei Notebooks nicht vorgenommen. Für die USB-Sticks existiert seit 2010 ein „Merkblatt für die Nutzung digitaler Speichermedien. Es werden ausschließlich passwortgeschützte U3-USB-Sticks ausgegeben. Der Anwender erhält zudem das v.g. Merkblatt, in dem das Verfahren beschrieben wird. Zusätzlich beinhaltet der Stick ein separates Verschlüsselungsprogramm, falls sensible Daten im „ungeschützten“ Bereich des Sticks hinterlegt werden sollen.
MdJ	Neben den geräteabhängigen Sicherheitsmechanismen steht den Nutzern für die Verschlüsselung von Laptops und externen Datenträgern auf Anforderung PGP bzw. das Open-Source-Programm TrueCrypt zur Verfügung. Auf vielen Laptops werden lokal keine Daten gespeichert, da nur remote über VPN auf den Dienst-PC bzw. zentrale Server zugegriffen wird.

Wird bei dienstlichen Smartphones bei Verlust oder Diebstahl von der Möglichkeit der Datenlöschung durch Fernwartung Gebrauch gemacht?

#### Zu Frage 7:

Hinsichtlich der sicheren Anbindung mobiler Endgeräte ist festzuhalten, dass Vertreter des Unabhängigen Datenschutzzentrums in der entsprechenden Arbeitsgruppe des IT-Innovationszentrums mitgearbeitet und hier die Verschlüsselung und das Remote-Wiping thematisiert haben. So sind in der zentralen Blackberry-Infrastruktur viele Sicherheitsanregungen des Unabhängigen Datenschutzzentrums umgesetzt.

Die ZDV-Saar bietet den Ressorts die Nutzung der zentralen Blackberry-Infrastruktur an, mit der eine Sperrung bzw. Datenlöschung aus der Ferne möglich ist. In einigen Ressorts kann bei dienstlichen Smartphones von der Möglichkeit der Datenlöschung durch Fernwartung Gebrauch gemacht werden. Der Verlust von mobilen Endgeräten ist unverzüglich anzuzeigen.

Darüber hinaus werden in einzelnen Ressorts auch andere Endgeräte eingesetzt; dies erfolgt in der eigenen Zuständigkeit und Verantwortung des jeweiligen Ressorts. Sofern von diesen Geräten unterstützt – z.B. bei Apple Geräten – kann auch hier – unabhängig von der Blackberry-Infrastruktur – das Löschen von Geräten im Verlustfall aus der Ferne initiiert werden. Im Umweltministerium wird bei iPhones die Möglichkeit des Fernlöschens von Daten nicht praktiziert, da aus Sicherheitsgründen sowohl WLAN als auch GPS (Wahrung der Persönlichkeitsrechte durch Ortung) grundsätzlich deaktiviert sind.

Beim IT-Innovationszentrum laufen derzeit Planungen für die sichere Anbindung und Verwaltung weiterer mobiler Endgeräte über die v.g. zentrale Blackberry-Infrastruktur hinaus.

Müssen solche Verluste oder Diebstähle gemeldet werden? Falls ja, zu wie vielen Verlusten bzw. Diebstählen ist es in den vergangenen 10 Jahren gekommen? Bitte nach Jahren und betroffenen Ministerien bzw. Behörden aufschlüsseln inklusive einer Angabe, welche Daten von einem Verlust bzw. Diebstahl betroffen waren.

Zu Frage 8:

Verluste oder Diebstähle mobiler Endgeräte müssen unverzüglich gemeldet werden. An zentraler Stelle (ZDV-Saar, IT-Innovationszentrum) sind bisher keine Verluste von dienstlichen Smartphones bekannt.

<b>Ressort</b>	<b>Verluste oder Diebstähle dienstlicher mobiler Endgeräte wie z.B. Smartphones - Anzahl der Geräte -</b>
CdS	In den letzten 10 Jahren kam es zu keinen Verlusten
MfIS	Bisher sind keine Verlustmeldungen eingegangen.
MFE	Bisher sind keine Verlustmeldungen eingegangen.
MfSGFF	In den letzten 10 Jahren kam es zu keinen Verlusten.
MBK	Bisher sind keine Verlustmeldungen eingegangen.
MfWAEV	Bisher sind keine Verlustmeldungen eingegangen.
MfUV	Bei der Übergabe eines digitalen Datenträgers (Notebook, USB-Stick, Smartphone) erhält der Benutzer ein Merkblatt und beim Mobiltelefon eine Checkkarte, auf dem/der sich alle notwendigen Informationen befinden, um einen Verlust an alle zuständigen Stellen zu melden (Deaktivierung, Netz-/Exchange-Zugang, Löschen Zugang beim Provider). Verluste von Smartphones sind keine zu verzeichnen.
MdJ	Bisher sind keine Verlustmeldungen eingegangen.

Ergänzend wird darauf hingewiesen, dass im Rahmen des Projektes „IT-Neuausrichtung“ eine ressortübergreifende Facharbeitsgruppe Informationssicherheit eingerichtet wurde. Dieses Kompetenzteam hat die Aufgabe, einheitliche Standards der IT-Sicherheit für alle Ressorts zu entwickeln.