Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Leitfaden über Internet- und E-Mailüberwachung am Arbeitsplatz

Für die Bundesverwaltung

Stand: September 2013

Feldeggweg 1, 3003 Bern
Tel. 058 462 43 95, Fax 058 465 99 96
www.edoeb.admin.ch

Inhaltsverzeichnis

1. Einleitung: Das Überwachen von E-Mail-Verkehr und Internetnutzung

Dieser Leitfaden zeigt den Bundesangestellten auf, wie und zu welchen Zwecken ihr E-Mail-Verkehr und ihre Internetnutzung überwacht werden dürfen, und er erläutert den Bundesorganen, welche E-Mail-Verkehr und die Internetnutzung der angestellten Personen überwachen wollen, welche gesetzlichen Bestimmungen zu beachten sind. Besonders wird hier auf die seit dem 1. April 2012 in Kraft getretenen Bestimmungen des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG) und der neu geschaffenen Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (SR 172.010.442), eingegangen. Da dieser Verordnung keine offizielle Abkürzung zugeteilt wurde, wird sie im Weiteren für eine verbesserte Lesbarkeit als «Randdatenverordnung» bezeichnet.

Zunächst gilt festzuhalten, dass innerhalb der Bundesverwaltung bis zum 1. April 2012 keine Bestimmungen bestanden haben, welche die Aufzeichnung oder Auswertung der beim Mailen oder Surfen anfallenden Randdaten regelten. Allfällige Nutzungsbestimmungen einzelner Bundesorgane, die bereits vor dem 1. April 2012 zur Anwendung gelangten, hatten somit keine gesetzliche Grundlage und müssen jetzt auf ihre Vereinbarkeit mit den Bestimmungen des RVOG und der Randdatenverordnung überprüft werden.

Zudem muss beachtet werden, dass die neuen Bestimmungen nur eine Überwachung ex post (im Nachhinein) zulassen. Für eine Echtzeitüberwachung mit entsprechenden Programmen oder Geräten (Keylogger) bilden die neuen Bestimmungen keine gesetzliche Grundlage (siehe dazu Ziffer 6, Überwachungsprogramme).

2. Tangierte Interessen des Arbeitgebers

Durch Surfen und Mailen am Arbeitsplatz können bestimmte Interessen des Arbeitgebers beeinträchtigt und die technische Einrichtung gefährdet werden. Beispiele sind:

- Speicherkapazität und Netzwerkdurchsatz (Reduktion der Datenflusskapazität) durch übermässiges Surfen und Mailen;
- Daten- und Anwendungssicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) durch Einlass von Viren, Würmern, Trojanern oder durch Installation von fremden Programmen;
- Arbeitszeit und andere finanzielle Interessen (Produktivitätsverringerung oder -verlust, Kostensteigerung durch zusätzlichen Aufwand);
- Weitere rechtlich geschützte Interessen des Arbeitgebers wie Ruf, Fabrikations- und Geschäftsgeheimnisse oder Datenschutz.

3. Die Randdaten

Beim Surfen und Mailen bleiben an verschiedenen Ort Spuren erhalten, die sogenannten Randdaten. In der Regel führen gemeinsam benutzte Informatikmittel (z. B. Server) eine Protokollierung der durchgeführten Aktivitäten aus. Sie erstellen sogenannte Logfiles, in welchen die Randdaten enthalten sind.

Normalerweise werden beim Surfen und Mailen nur die Randdaten, also wer wann was getan hat, aufgezeichnet. Für Sicherungszwecke (Backups) dürfen bei E-Mails aber auch die Inhalte gespeichert werden.

Die für die Überwachung der Mitarbeiterinnen und Mitarbeiter relevanten Protokollierungen können hauptsächlich an vier verschiedenen Stellen erfolgen: Auf dem Computer des Benutzers, auf Intranet-Servern, auf Netzkopplungselementen (Firewall oder Router) und auf DMZ-Servern (siehe unten).

Auf Intranet-Servern wie Domäne-Servern besteht die Protokollierung aus Benutzername (wer), Datumsangaben (wann), Handlungen (Ein- und Ausloggen), dynamische IP-Adressenvergabe, DNS-Adressenauflösung (Domain Name System) und Applikationsaufruf (was).

Eine «demilitarisierte Zone» (DMZ) zwischen Intranet und Internet wird oft von Firewalls geschützt, um von beiden Zonen zugreifbare Server beherbergen zu können. Es handelt sich meistens um die E-Mail-, File- und Webserver.

Auf den E-Mail-Servern werden u. A. Zeitangaben, Absender- und Empfängeradresse, Betrefftext, Priorität und Vertraulichkeit der Nachricht protokolliert. Es können aber auch weitere Daten protokolliert werden (z. B. Anzahl Attachements, Grösse des E-Mails, digitale Signatur, ev. auch IP-Adresse).

4. Gesetzliche Grundlagen für die Überwachung

Neben den Bestimmungen des RVOG und der Randdatenverordnung kommt auch das Bundesgesetz über den Datenschutz (DSG) zur Anwendung. Die hier erläuterte Auswertung der Logdateien (Randdaten) stellt eine Bearbeitung von Personendaten gemäss Artikel 3 Buchstabe e DSG dar, wenn die Randdaten vor der Auswertung nicht anonymisiert werden. Bundesorgane dürfen gemäss Artikel 17 Absatz 1 DSG Personendaten nur bearbeiten, wenn dafür eine gesetzliche Grundlage besteht. Vorliegend besteht diese aus den betreffenden Bestimmungen des RVOG oder der Randdatenverordnung. Vorbehalten sind, nach Artikel 57i RVOG weitere Bestimmungen des Bundesrechts. Zudem müssen bei der Bearbeitung von Personendaten die allgemeinen Datenschutzbestimmungen der Artikel 4ff. DSG berücksichtigt werden. Dazu gehören insbesondere die Grundsätze der Verhältnismässigkeit, der Zweckbindung und der Transparenz. Bevor die spezialgesetzlichen Bestimmungen erläutert werden, wollen wir hier kurz diese Grundsätze des Datenschutzrechts in Erinnerung rufen.

4.1 Die Verhältnismässigkeit

Artikel 4 Absatz 2 DSG hält fest, dass eine Bearbeitung von Personendaten verhältnismässig sein muss. In Bezug auf die Auswertung der Randdaten bedeutet das, dass nur diejenigen Auswertungen vorgenommen werden dürfen, welche für das Aufdecken von Missbräuchen, zur Behebung von Störungen oder zur Abwehr von konkreten Bedrohungen geeignet sind. Weiter hat das Bundesorgan respektive die Betreiberin der elektronischen Infrastruktur dabei diejenigen Auswertungsform zu wählen, welche den mildesten Eingriff in die Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter darstellt.

4.2 Zweckbindung

Der Grundsatz der Zweckbindung (Artikel 4 Absatz 3 DSG) bedeutet, dass die Randdaten nur für diejenigen Zwecke verwendet werden dürfen, welche gesetzlich vorgesehen sind. Werden die Logdateien durch das Bundesorgan oder durch die Betreiberin der elektronischen Infrastruktur für einen Zweck ausgewertet, der nicht im Gesetz vorgesehen ist, so stellt das einen Verstoss gegen den Grundsatz der Zweckbindung und somit gegen das RVOG und das Datenschutzgesetz dar.

4.3 Transparenz

Im Gegensatz zur Überwachung im Bereich der Privatwirtschaft kann sich das Bundesorgan oder die Betreiberin darauf berufen, dass Mitarbeiterinnen und Mitarbeiter der Bundesverwaltung die gesetzlichen Bestimmungen kennen. Ein Überwachungsreglement muss durch das Bundesorgan im Prinzip also nicht erstellt werden. Dem Grundsatz der Transparenz (Artikel 4 Absatz 4 DSG) muss das Bundesorgan aber durch den Erlass des Nutzungsreglements nachkommen. Aufgrund der Definition des Missbrauchs kommt somit neu dem Nutzungsreglement eine absolut zentrale Bedeutung zu. Weiter wird auch durch die Bekanntgabe des Auswertungsergebnisses für Transparenz gesorgt.

5. Verbot der Verhaltensüberwachung

Auch innerhalb der Bundesverwaltung gilt Artikel 26 Absatz 1 der Verordnung 3 zum Arbeitsgesetz (ArGV 3). Die Verhaltensüberwachung der Mitarbeiterinnen und Mitarbeiter mit Überwachungs- und Kontrollsystemen ist verboten. Ziel dieser Bestimmung ist der Gesundheitsschutz. Werden Überwachungs- und Kontrollsysteme für andere Zwecke eingesetzt, so sind sie zulässig, wenn sie so ausgestaltet sind, dass die Gesundheit und die Bewegungsfreiheit der Mitarbeiterinnen und Mitarbeiter nicht beeinträchtigt werden.

Für das Surfen und Mailen am Arbeitsplatz bedeutet das, dass das ständige personenbezogene Auswerten der Logdaten nicht zulässig ist.

Der Einsatz von Key-Loggern und anderen Überwachungsprogrammen, welche jede Tätigkeit der Mitarbeiterin oder des Mitarbeiters am Computer erfassen, ist ohne richterliche Anweisung auch aufgrund von Artikel 26 Absatz 1 ArGV 3 verboten.

Auch sogenannte Content Scanner, welche jedes gesendete oder erhaltene E-Mail auf vordefinierte Stichwörter untersuchen und entsprechend reagieren (Sperrung/Löschung der E-Mail, Benachrichtigung des Systemadministrators oder auch der vorgesetzten Person) werden eingesetzt. Der Nutzen dieser Programme ist umstritten, da die Belegschaft sich mit diesen Programmen quasi «arrangieren» und sie durch das Ausschreiben von Spezialzeichen oder durch eine verklausulierte Sprache umgehen kann. Wird jedes E-Mail mittels Content Scanner bearbeitet, so stellt sich auch hier die Problematik der verbotenen Verhaltensüberwachung (siehe auch Ziffer 6).

6. Überwachungsprogramme

Für den Einsatz von auf dem Computer der Mitarbeiterin oder des Mitarbeiters installierten Überwachungsprogrammen bilden die neuen Bestimmungen des RVOG keine genügende gesetzliche Grundlage. Derartige Überwachungsprogramme können wie im privaten Bereich aufgrund des massiven Eingriffs in die Persönlichkeitsrechte der Mitarbeiterin oder des Mitarbeiters nur aufgrund einer richterlichen Anweisung eingesetzt werden.

Direkt auf dem Computer installierte Überwachungsprogramme lassen eine detaillierte Überwachung sämtlicher Aktivtäten zu. Sie erlauben Einsicht in E-Mails oder stellen in regelmässigen Zeitabständen Screenshots her. Mit Keyloggern können sämtliche Tastenanschläge erfasst werden. Da Überwachungsprogramme systematisch die Aktivitäten der Mitarbeiterin oder des Mitarbeiters erfassen, stellt deren Einsatz ohne richterliche Anordnung einen Verstoss gegen das Verbot der Verhaltensüberwachung dar (siehe Ziffer 5).

7. Technische und organisatorische Massnahmen

Auch Bundesorgane müssen sich, bevor sie eine personenbezogene Überwachung der Mitarbeiterinnen und Mitarbeiter durchführen, die Frage stellen, welche technischen und organisatorischen Massnahmen sie zur Verhinderung von Missbräuchen ergriffen haben oder noch ergreifen können.

Klarerweise müssen die Bundesorgane ihren Mitarbeiterinnen und Mitarbeiter gegenüber kommunizieren, welche Nutzung von E-Mail und Internet erlaubt ist, respektive welche Nutzungen nicht akzeptiert werden. Dafür erlässt das Bundesorgan ein Nutzungsreglement, welches den Mitarbeiterinnen und Mitarbeitern bekannt gegeben wird. Dieses spielt mit den neuen Bestimmungen ohnehin eine zentrale Rolle, da der Begriff des Missbrauchs grundsätzlich als Verletzung der Nutzungsbestimmungen qualifiziert wird (siehe Ziffer 9, Der Missbrauch).

7.1 Technische Massnahmen

Zu den wichtigsten technischen Massnahmen gehören Authentifizierung und Autorisierung, Verschlüsselungsanwendungen, Antivirenprogramme, Discquotamanager, Backups und Firewalls. Selbstverständlich müssen Mail- und Surfprogramme nach dem aktuellsten Stand der Technik konfiguriert und regelmässig aktualisiert werden.

Im Bereich **Authentifizierung** sollte eine Lösung mit zwei Faktoren (Passwort und bspw. Smartcard) implementiert sein. Die **Autorisierung** stellt sicher, dass der Zugriff auf bestimmte Daten nur denjenigen Personen möglich ist, die diese Daten für die Erledigung ihrer Aufgabe tatsächlich benötigen. Dies kann mittels Rollen- und Berechtigungskonzept erreicht werden.

Verschlüsselungsanwendungen sind einzusetzen, um sicherzustellen, dass vertrauliche oder besonders schützenswerte Personendaten oder Persönlichkeitsprofile nur durch die berechtigten Personen bearbeitet werden können. Dazu gehören zum Beispiel Secure Messaging, Secure Center und BitLocker.

Discquotamanager sind Programme, welche die Speicherkapazität (Files und Mailboxen) jeder Benutzerin oder Benutzers begrenzen. Discquotamanager vermeiden unnötige Auslastungen der Speicherkapazität.

Firewalls schützen die Daten vor externen Angriffen und verhindern, dass Netzwerkbandbreite und Arbeitszeit übermässig beansprucht werden. Die Firewall kann mit einer Sperrliste erweitert werden. Diese enthält Internetadressen, welche durch Mitarbeiterinnen und Mitarbeiter nicht aufgerufen werden dürfen. Auch eine Positivliste (Liste mit den erlaubten Internetseiten) ist möglich.

Auch **bestimmte Dateiformate** (.exe, .mp3, .bat) können für den Download gesperrt werden. Dies ist aber nur eine begrenzt effektive Massnahme, da z. B. komprimierte Archivdateien (zip) gesperrte Dateien enthalten können.

7.2 Organisatorische Massnahmen: Das Nutzungsreglement

Die wichtigste organisatorische Massnahme stellt der Erlass eines Nutzungsreglements dar. Darin bestimmen die Bundesorgane, wie Mitarbeiterinnen und Mitarbeiter Internet und E-Mail für berufliche und nicht-berufliche Zwecke nutzen dürfen. Das Nutzungsreglement hat mit den neuen RVOG-Bestimmungen eine zentrale Bedeutung erhalten, da das Bundesorgan hier auch festhält, welches Verhalten als Missbrauch betrachtet wird.

Das Nutzungsreglement schafft Transparenz und Rechtssicherheit. Es verhindert so auch unnötige Diskussionen zwischen Bundesorgan und Arbeitnehmerin oder Arbeitnehmer. Das Reglement ist der Belegschaft bekannt zu geben. Üblicherweise geschieht dies in schriftlicher Form. Aus Beweisgründen lässt sich das Bundesorgan vorteilhafterweise den Erhalt von den Mitarbeiterinnen und Mitarbeitern quittieren. Grosse Dienststellen geben den Mitarbeiterinnen und Mitarbeitern das Nutzungsreglement üblicherweise elektronisch bekannt. Oftmals erhalten die Mitarbeiterinnen und Mitarbeiter ein E-Mail mit dem Link zum Nutzungsreglement, welches im Intranetbereich des Bundesorgans abrufbar ist. Auch diese Vorgehensweise ist zulässig. Anpassungen des Reglements hat das Bundesorgan der Belegschaft zu kommunizieren.

Ein Nutzungsreglement kann für ein ganzes Departement erlassen werden und hat dann Gültigkeit für alle Mitarbeiterinnen und Mitarbeiter. Oftmals erlassen Bundesämter oder Dienststellen aber eigene Nutzungsreglemente. Dies macht besonders dort Sinn, wo Mitarbeiterinnen und Mitarbeiter für das Erfüllen ihrer beruflichen Aufgaben das Internet oder auch das E-Mail in einer Art und Weise benützen müssen, die von der im Departement ansonsten bewilligten Nutzung abweicht. Grundsätzlich kann festgehalten werden, dass für die Mitarbeiterinnen und Mitarbeiter das Nutzungsreglement gilt, welches ihnen bekannt gemacht wurde (Grundsatz der Transparenz).

Normalerweise gestattet das Bundesorgan der Belegschaft die private Nutzung von Internet und E-Mail in beschränktem Ausmass. Zum Beispiel wird das Surfen erlaubt, solange das Erfüllen der arbeitsvertraglichen Verpflichtungen nicht behindert wird. Je nach Tätigkeitsbereich kann aber auch ein totales Verbot für privates Mailen und Surfen angezeigt sein. Ein Bundesorgan, das ein solches Totalverbot anordnet, muss sich aber bewusst sein, dass das Durchsetzen bzw. die Kontrolle des Verbots mit einem sehr grossen Aufwand verbunden ist.

Zusammenfassend kann festgehalten werden: Je klarer das Nutzungsreglement ist, desto besser weiss die Belegschaft, was erlaubt und was verboten ist. Unnötige Streitigkeiten werden so verhindert.

8. Die Aufzeichnung der Randdaten

Artikel 57l RVOG regelt, für welche Zwecke die Randdaten, bei E-Mails auch deren Inhalt, aufgezeichnet werden dürfen. Der E-Mail-Inhalt darf von Bundesorganen allerdings nur für die Sicherung (Backup) aufgenommen werden. Er ist also im Rahmen der Nutzungsüberwachung nicht zugänglich.

Die Randdaten, welche beim Surfen und Mailen anfallen, dürfen gemäss Artikel 57l Buchstabe b RVOG für verschiedene Zwecke aufgezeichnet werden. Hier relevant sind lediglich die Ziffern 1, 2 und 3 der besagten Bestimmung. Die zulässigen Zwecke sind:

- die Aufrechterhaltung der Informations- und Dienstleistungssicherheit;
- die technische Wartung der elektronischen Infrastruktur;
- die Kontrolle der Einhaltung des Nutzungsreglements.

9. Der Missbrauch

Der Missbrauch ist in Artikel 10 Absatz 1 Randdatenverordnung definiert. Ein Missbrauch liegt dann vor, wenn die Art oder das Ausmass der Nutzung die Vorgaben des Bundesorgans oder Rechtsvorschriften verletzt. Hier zeigt sich die Wichtigkeit des Erlasses von Nutzungsbestimmungen in Form eines Nutzungsreglements durch das Bundesorgan. Besteht kein solches Reglement, so kann das Bundesorgan nur den Verstoss gegen Rechtsvorschriften als Missbrauch und somit als Grundlage für eine personenbezogene namentliche Auswertung geltend machen.

Grundsätzlich können zwei Arten von Missbrauch unterschieden werden:

1. **Quantitativer Missbrauch**: Die Mitarbeiterin oder der Mitarbeiter surft und mailt übermässig für private Zwecke. Ressourcen und Mittel des Bundesorgans werden missbraucht.
2. **Qualitativer Missbrauch**: Beim Surfen werden Internetseiten mit illegalen oder mit vom Bundesorgan als unerlaubt definierten Inhalten aufgerufen. Auch Mobbing per E-Mail stellt beispielsweise einen qualitativen Missbrauch dar.

10. Auswertungsformen

Grundsätzlich bestehen drei Formen der Auswertung der Randdaten. Entsprechend dem Prinzip der Verhältnismässigkeit muss das Bundesorgan immer diejenige Form wählen, die für den angestrebten Zweck (das Verhindern bzw. Aufdecken von Missbräuchen) geeignet ist und den schwächsten Eingriff in die Persönlichkeitsrechte der betroffenen Person darstellt. Die drei Formen sind:

10.1 Nicht personenbezogene (anonyme) Auswertung: Artikel 57m RVOG, Artikel 8 Randdatenverordnung

Logdateien sind personenbezogen, da sie konkrete Angaben zu der Person machen, welche sie verursacht hat. Es kann sich dabei um die E-Mail-Adresse, die IP-Adresse oder eine Kennnummer der Mitarbeiterin oder des Mitarbeiters handeln. Die anonyme Auswertung der Randdaten bedeutet aber nicht, dass die Daten vor der Auswertung anonymisiert werden müssen. Die Ergebnisse der Auswertung werden in rein statistischer Form, ohne Personenbezug und somit anonym, dargestellt. Eine mögliche ano-

nyme Auswertung kann zum Beispiel sein: Wie viele Internetseiten mit pornographischem Inhalt werden durch die Belegschaft pro Monat angesurft? Diese Auswertungen können zeitlich und sachlich unbeschränkt für alle in Artikel 57l RVOG genannten Zwecke durchgeführt werden. Zentraler Zweck ist hier, die Einhaltung des Nutzungsreglements zu kontrollieren (Artikel 57l Buchstabe b Ziffer 3 RVOG).

10.2 Nicht namentliche personenbezogene (pseudonyme) Auswertung: Artikel 57n RVOG, Artikel 9 Randdatenverordnung

Wiederum gilt zu bedenken, dass die Logdateien einen mehr oder weniger direkten Bezug zur Person aufweisen können. Entweder enthalten sie direkt den Namen der Mitarbeiter (E-Mail) oder eine IP-Adresse/Kennnummer (Internet). Für eine nicht namentliche personenbezogene Auswertung muss somit im Resultat der Auswertung der direkte Personenbezug durch die Vergabe von Pseudonymen verhindert werden. Eine solche Auswertung beantwortet zum Beispiel die Frage: Gibt es in einer bestimmten Abteilung Mitarbeiterinnen oder Mitarbeiter, welche pro Woche mehr als 100 E-Mails versenden? Wer dieses Kriterium erfüllt, wird, mit einem Pseudonym versehen, aufgelistet. Diese Auswertung darf **nur stichprobenweise (also nicht systematisch)** zur Kontrolle der Nutzung der elektronischen Infrastruktur vorgenommen werden (Artikel 57n Buchstabe a RVOG). Es muss somit kein Verdacht auf einen Missbrauch vorliegen.

10.3 Namentliche personenbezogene Auswertung: Artikel 57o RVOG, Artikel 10 und 11 Randdatenverordnung

Hier wird das Resultat der Auswertung der Randdaten konkret bezogen auf eine oder mehrere Personen dargestellt. Diese Auswertung beantwortet zum Beispiel die Frage: Welche Mitarbeiterinnen und Mitarbeiter surfen pro Tag mehr als zwei Stunden? Das Resultat wird mit identifizierenden Merkmalen (Name, Kennnummer oder andere im Bundesorgan verwendete Identifikatoren) dargestellt. Die namentliche personenbezogene Auswertung ist zulässig, um einen konkreten Verdacht auf Missbrauch der elektronischen Infrastruktur abzuklären und einen erwiesenen Missbrauch zu ahnden (Artikel 57o Absatz 1 Buchstabe a RVOG). Hier zeigt sich die zentrale Bedeutung des Nutzungsreglements, in dem konkret die Missbräuche definiert sind.

10.4 Wer wertet aus?

Hier werden zunächst einige Begriffe der neuen Bestimmung von RVOG und Randdatenverordnung geklärt.

Grundsätzlich können Auswertungen durch

- die Betreiberin,
- die nach dem Datenschutzkonzept des Bundesorgans vorgesehene Stelle oder
- das Bundesorgan

durchgeführt respektive angeordnet werden.

Damit insbesondere die weiteren Ausführungen zu den Auswertungsvoraussetzungen klar sind, muss festgehalten werden:

Betreiberin ist, gemäss Artikel 1 Buchstabe c Randdatenverordnung, die mit dem technischen Betrieb der elektronischen Infrastruktur des Bundes beauftragte Stelle. In Zusammenhang mit E-Mail und Inter-

net ist dies meistens das Bundesamt für Informatik und Telekommunikation (BIT). Bestimmte Departemente, zum Beispiel das VBS, betreiben jedoch ein eigenes Rechenzentrum für diese Aufgaben.

Die **nach dem Datenschutzkonzept des Bundesorgans vorgesehene Stelle** ist in der Regel die Datenschutzberaterin oder der Datenschutzberater des Bundesorgans.

Als **Bundesorgane** gelten Behörden und Dienststellen des Bundes (Departemente, Ämter, Bundeskanzlei, dezentralisierte Verwaltungseinheiten, eidgenössische Anstalten etc.) sowie natürliche und juristische Personen ausserhalb der Bundesverwaltung, soweit sie mit öffentlichen Aufgaben des Bundes betraut sind (wie etwa Post, SBB und SUVA).

Bewirtschaftete Daten gemäss Artikel 1 Buchstabe a Randdatenverordnung sind Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes aufgezeichnet und regelmässig genutzt, ausgewertet oder bewusst gelöscht werden. Vereinfacht gesagt: Bewirtschaftete Daten (Randdaten) fallen dort an, wo Geräte in einem Netzwerkverbund betrieben werden.

Nicht bewirtschaftete Daten sind gemäss Artikel 1 Buchstabe b der Randdatenverordnung Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes aufgezeichnet, aber nicht regelmässig genutzt, ausgewertet oder bewusst gelöscht werden. Für die Überwachung der E-Mail- und Internetnutzung sind diese Daten nicht relevant, da bei E-Mail- und Internetnutzung innerhalb der Bundesverwaltung grundsätzlich immer bewirtschaftete Randdaten entstehen. Eine Ausnahme könnte nur dann auftreten, wenn ein Bundesorgan bewusst technische Vorkehrungen trifft, die das verhindert. Als erklärendes Beispiel für eine Nutzung der elektronischen Infrastruktur, welche dazu führt, dass nicht bewirtschaftete Randdaten entstehen, ist ein Fotokopierer, der nicht an ein Netzwerk angeschlossen ist. Der Fotokopierer verfügt über ein internes Speichermedium, worauf verschiedene Nutzungsdaten (Datum, Zeit, Seitenzahlen, etc.) gespeichert werden. Wenn die Speicherkapazität erreicht ist, erfolgt bei weiteren Kopiervorgängen eine Überschreibung der alten Nutzungsdaten. Nach dem Überschreiben stehen die alten Randdaten nicht mehr zur Verfügung und können deshalb auch nicht mehr ausgewertet werden.

11. Auswertungsvoraussetzungen

Entsprechend der Intensität des Eingriffs in die Persönlichkeitsrechte der Mitarbeiterinnen und Mitarbeiter gelten für die drei dargestellten Auswertungsformen unterschiedlich hohe Anforderungen. Diese sind in der Randdatenverordnung festgehalten. Hier sei der Hinweis erlaubt, dass das Auswerten der Randdaten eine sehr aufwendige und damit auch teure Angelegenheit darstellen kann. Jedes Bundesorgan wird sich deshalb in der Praxis nicht nur die Frage stellen müssen, ob die Voraussetzungen für die gewünschte Auswertung gegeben sind, sondern auch, ob es die Kosten einer Auswertung rechtfertigen kann.

11.1 Nicht personenbezogene Auswertung: Artikel 8 Randdatenverordnung

Die **Betreiberin** und **die nach dem Datenschutzkonzept des Bundesorgans vorgesehene Stelle** können nicht personenbezogene Auswertungen von bewirtschafteten Daten für alle in Artikel 57l Buchstabe b RVOG vorgesehenen Zwecke vornehmen. Diese Auswertung kann systematisch und ohne konkreten Anlass erfolgen (zeitlich und sachlich unbeschränkt).

Hier stellt sich die Frage, ob diese Form der Auswertung auch durch **das Bundesorgan** angeordnet werden kann. Eine rein grammatische Auslegung der gesetzlichen Bestimmungen würde dazu führen,

dass sie, im Gegensatz zur nicht namentlichen personenbezogenen Auswertung, nur durch die Betreiberin und die nach Datenschutzkonzept des Bundesorgans vorgesehene Stelle durchgeführt werden kann. Richtigerweise muss diese Form der Auswertung aber auch **durch das Bundesorgan angeordnet** werden können. Die Unterscheidung der Durchführungsberechtigten respektive der Antragsberechtigten soll nur eine Differenzierung zur namentlichen personenbezogenen Auswertung gemäss Artikel 10 herstellen (siehe hierzu unten).

11.2 Nicht namentliche personenbezogene Auswertung: Artikel 9 Randdatenverordnung

Von sich aus können

- die Betreiberin,
- die nach dem Datenschutzkonzept des Bundesorgans vorgesehene Stelle oder
- das Bundesorgan

die bewirtschafteten Daten gemäss Artikel 57n Buchstabe a und b RVOG **stichprobenartig** zur Kontrolle der Nutzung der elektronischen Infrastruktur und zur Kontrolle der Arbeitszeiten des Personals auswerten. Diese Form der Auswertung kann auch vom Bundesorgan angeordnet werden. Es ist aber zu betonen, dass die nicht namentliche personenbezogene Auswertung **nicht systematisch** durchgeführt werden darf.

In der Praxis dürfte nun der Fall auftreten, dass eine nicht namentliche personenbezogene Auswertung aufzeigt, dass bei einer bestimmten Mitarbeiterin oder einem bestimmten Mitarbeiter oder auch bei einer ganzen Gruppe von Mitarbeiterinnen und Mitarbeitern ein Missbrauch vorliegen könnte. Es stellt sich nun die Frage, ob dieser Anfangsverdacht als Grundlage für eine namentliche personenbezogene Auswertung dienen kann. Wie so oft im Bereich des Datenschutzes kann diese Frage nicht allgemeingültig beantwortet werden. Vielmehr ist festzuhalten, dass auf jeden Fall ein ausreichend konkretisierter Verdacht des Missbrauchs bestehen muss und dass die namentliche personenbezogene Auswertung unter Einbezug der konkreten Sachverhaltsmomente verhältnismässig zu sein hat. Zudem gilt es zu bedenken, dass eine derartige Auswertung erhebliche finanzielle Mittel beansprucht.

11.3 Namentliche personenbezogene Auswertung: Artikel 10, 11, 12 und 13 Randdatenverordnung

Da die namentliche personenbezogene Auswertung der Randdaten den intensivsten Eingriff in die Persönlichkeitsrechte der Angestellten darstellt, wurden hier auch die Anforderungen besonders hoch angesetzt. Dies zeigt sich darin, dass die Anforderungen an den Auftrag für diese Auswertung in der Randdatenverordnung ausdrücklich geregelt sind, dass zwischen drei verschiedenen Auswertungszwecken (mit unterschiedlichen Voraussetzungen) unterschieden wird, und dass sie nur durch Bundesorgane und nach einer schriftlichen Information der betroffenen Person durchgeführt werden darf.

Die zulässigen Zwecke der namentlichen personenbezogenen Auswertung sind in Artikel 57o Absatz 1 RVOG genannt.

11.3.1 Auftrag für die namentliche personenbezogene Auswertung wegen Missbrauchs oder Missbrauchsverdachts: Artikel 10 Randdatenverordnung

Die Auswertung darf nur durch das Bundesorgan, für das die Nutzerin oder der Nutzer der elektronischen Infrastruktur arbeitet, selbst durchgeführt oder angeordnet werden. Bundesorgane, die einen externen (nicht der Bundesverwaltung angehörenden) Betreiber haben, dürfen somit die Auswertung nicht durch diesen durchführen lassen. Die vertragliche Regelung zwischen dem Bundesorgan und dem Dienstleister (Auftragsdatenbearbeiter) macht letzteren nicht zu einem Bundesorgan. Der EDÖB lehnt die juristische Konstruktion, dass es sich beim externen Dienstleister um eine Hilfsperson des Bundesorgans handelt, ab. Will ein Bundesorgan, das sich in dieser Situation befindet, die Randdaten also namentlich personenbezogen auswerten und kann oder darf das nicht selber, muss es die Logfiles zur Auswertung an ein Bundesorgan übergeben, das die entsprechenden Möglichkeiten hat.

Vor dieser Auswertung muss die betroffene Person schriftlich informiert werden (Artikel 57o Absatz 2 Buchstabe b RVOG). Stimmt sie nicht zu, so muss die Leitung des Bundesorgans die Auswertung bewilligen. Wer diesem Gremium angehört, muss jedes Bundesorgan definieren.

Falls das auftraggebende Bundesorgan über eine Datenschutzberaterin oder einen Datenschutzberater verfügt, so muss sie/er **zwingend** eine Kopie des Auswertungsauftrages erhalten (Artikel 10 Absatz 3 Randdatenverordnung).

11.3.2 Durchführung der namentlichen personenbezogenen Auswertung wegen Missbrauchs oder Missbrauchsverdachts: Artikel 11 Randdatenverordnung

Vor der Auswertung muss das beauftragte Bundesorgan (in der Regel das BIT) prüfen, ob der konkrete Missbrauchsverdacht hinreichend schriftlich begründet oder der Missbrauch belegt ist (Artikel 11 Absatz 1 Buchstaben a und b Randdatenverordnung). Zudem muss es überprüfen, ob die betroffene Person über den Missbrauchsverdacht bzw. Missbrauch schriftlich informiert worden ist. Aufgrund des Wortlauts von Artikel 57o Absatz 2 Buchstabe b RVOG muss auch kontrolliert werden, dass die betroffene Person über die bevorstehende Auswertung schriftlich informiert wurde.

Sollte sich das beauftragte Bundesorgan weigern, die Auswertung vorzunehmen, weil es der Meinung ist, dass die Voraussetzungen (konkreter, schriftlich begründeter Verdacht oder Missbrauch, schriftliche Information der betroffenen Person, Zustimmung der betroffenen Person respektive Bewilligung durch die Leitung des Bundesorgans) nicht erfüllt sind, kann das auftragserteilende Bundesorgan den EDÖB um eine Stellungnahme ersuchen.

Der EDÖB wird in einem solchen Fall überprüfen, ob die formellen Voraussetzungen für eine namentliche personenbezogene Auswertung erfüllt sind. Er wird seine Beurteilung in einer schriftlichen Stellungnahme den beteiligten Bundesorganen und der betroffenen Person zukommen lassen. Dabei handelt es sich nicht um eine formelle Entscheidung, da der EDÖB hierzu keine Kompetenz erhalten hat. Die Stellungnahme ist vielmehr eine Expertenmeinung, welche von den beteiligten Bundesorganen und auch der betroffenen Person im weiteren Verfahren verwendet werden kann.

Für den Fall, dass auftragserteilendes und durchführendes Bundesorgan identisch sind (etwa bei VBS, BIT und grundsätzlich überall dort, wo das Bundesorgan auch Betreiber der elektronischen Infrastruktur ist), wurde in Artikel 11 Absatz 3 Randdatenverordnung festgehalten, dass **die Datenschutzberaterin oder der Datenschutzberater des Departements** zwingend informiert werden muss.

11.3.3 Namentliche personenbezogene Auswertung zur Behebung von Störungen (und Abwehr von konkreten Bedrohungen): Artikel 12 Randdatenverordnung

Diese Auswertung der E-Mailnutzung oder des Surfverhaltens wird durchgeführt, um herauszufinden, welche Mitarbeiterin oder Mitarbeiter die Störung oder Bedrohung verursacht (hat). Konkret kann es zum Beispiel darum gehen festzustellen, welcher Mitarbeiter einen Trojaner in das System eingeschleppt hat und wie dies geschehen konnte, oder welche Mitarbeiterin durch Filesharing den Netzwerkdurchsatz verringert.

Diese Auswertung kann von der Betreiberin und von der Stelle, welche nach dem Datenschutzkonzept des Bundesorgans vorgesehen ist, **von sich aus** durchgeführt werden. Diese Regelung ist notwendig, damit gerade die Betreiberin, welche für die Funktionalität der Infrastruktur verantwortlich ist und technische Störungen beheben muss, auch ohne formellen Auftrag des Bundesorgans handeln kann. Damit die Betreiberin aber nicht leichtfertig von sich aus namentliche personenbezogene Auswertung durchführt, hält Artikel 12 Absatz 2 Randdatenverordnung fest, dass diese Auswertung nur zulässig ist, wenn sie,

1. erforderlich ist (mit einer anderen, weniger invasive Auswertungsform kann der Zweck nicht erreicht werden),
2. die Nutzung der elektronischen Infrastruktur wegen eines Defekts oder einer ausserordentlichen Beanspruchung durch Nutzerinnen oder Nutzer verunmöglicht oder stark eingeschränkt ist, oder
3. die unmittelbare Gefahr einer Schädigung der elektronischen Infrastruktur oder der Daten des Bundes besteht (Verbreitung von Schadprogrammen).

Nun muss hier klar festgehalten werden, dass eine namentliche personenbezogene Auswertung zur Überwachung der E-Mail- und Internetnutzung nicht einfach vorgenommen werden darf, wenn die Voraussetzungen von Artikel 10, 11 oder 12 Randdatenverordnung erfüllt sind. Es gelten weiterhin das Verhältnismässigkeitsprinzip und die weiteren Grundsätze des Datenschutzgesetzes (siehe: 4.1 - 4.3).

11.3.4 Information über das Auswertungsergebnis

Gemäss Artikel 15 Absatz 1 Randdatenverordnung übergibt die Betreiberin das Ergebnis der Auswertung dem auftragserteilenden Bundesorgan. Es muss im Fall einer namentlichen personenbezogenen Auswertung die betroffene Person zwingend über das Ergebnis der Auswertung informieren (Artikel 15 Absatz 2 Randdatenverordnung).