SWISS INFOSEC

Hacking Day - Datenschutz 2014

Betrachtung verschiedener rechtlicher Fragen

Reto C. Zbinden, Rechtsanwalt, Chief Executive Officer

SWISS INFOSEC

Datenschutzrechtliche Anforderungen und deren Umsetzung

Einführung

Datenschutz

Zweck und Begriffserläuterungen I

- Das Bundesgesetz über den Datenschutz (DSG) bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über welche Daten bearbeitet werden.
- Personendaten:
  - Alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.

Datenschutz

Zweck und Begriffserläuterungen II

Besonders schützenswerte Personendaten:

- die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
- die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
- Massnahmen der sozialen Hilfe,
- administrative oder strafrechtliche Verfolgungen und Sanktionen

Persönlichkeitsprofil:

- Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

Datenschutz- Registrierung einer Datensammlung

Datensammlung

- Bestand von Personendaten, der auf mehr als eine Person Bezug nimmt und nach betroffenen Personen erschlossen werden kann.
- Datensammlungen müssen beim EDÖB zur Registrierung angemeldet werden, wenn ohne gesetzliche Pflicht:
  - Entweder besonders schützenswerte Personendaten oder Bearbeitung von Persönlichkeitsprofilen oder
  - Bekanntgabe von Personendaten an Dritte.
- Diverse Ausnahmen von der Registrierungspflicht, u.a.
  - Wenn der Dateninhaber einen Datenschutzverantwortlichen bezeichnet hat, der unabhängig die betriebsinterne Einhaltung der Datenschutzvorschriften überwacht und ein Verzeichnis der Datensammlungen führt.

„Betrieblicher Datenschutzverantwortlicher“ Int. Datenschutzbeauftragter

- Inventar der Datensammlungen
- Überprüfung der Einhaltung des DSG
- Koordination des Auskunftsprozedere
- Erarbeitung und Durchsetzung der technischen und organisatorischen Massnahmen
- Periodische Kontrollen
- Ausbildung, Information und Sensibilisierung relevanter Stelle
- Förderung des integralen Sicherheitsdenkens

Auskunftsrecht 1/2

Jede Person kann vom Inhaber einer Datensammlung **Auskunft** darüber verlangen, **ob Daten über sie bearbeitet werden**.

Der Inhaber der Datensammlung muss ihr mitteilen:

- **alle über sie in der Datensammlung vorhandenen Daten**, einschliesslich der verfügbaren Angaben über die Herkunft der Daten;
- den **Zweck** und gegebenenfalls die **Rechtsgrundlagen** des Bearbeitens sowie
- die **Kategorien** der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger.

Daten über die **Gesundheit** kann der Inhaber der Datensammlung der betroffenen Person durch einen von ihr bezeichneten Arzt mitteilen lassen.

Auskunftsrecht 2/2

- Lässt der Inhaber der Datensammlung Personendaten durch einen **Dritten** bearbeiten, so bleibt er auskunftspflichtig. Der Dritte ist auskunftspflichtig, wenn er den Inhaber nicht bekannt gibt oder dieser keinen Wohnsitz in der Schweiz hat.
- Die Auskunft ist in der Regel **schriftlich**, in Form eines **Ausdrucks** oder einer Fotokopie sowie **kostenlos** zu erteilen. Der Bundesrat regelt die Ausnahmen.
- Niemand kann im Voraus auf das Auskunftsrecht verzichten.

Datenschutz

Outsourcing: Transfer ins Ausland

- Bei grenzüberschreitenden Bekanntgaben sind strenge Vorgaben zu beachten
- Das Gesetz listet abschliessend auf, unter welchen Voraussetzungen Personendaten an ausländische Staaten bekanntgegeben werden dürfen, wenn diese keine Datenschutzgesetzgebung kennen, die einen angemessenen Schutz gewährleistet.
- Bei der Beauftragung von Dritten muss sich der Auftraggeber über die Einhaltung der Sicherheitsmassnahmen vergewissern.

DSG Datensicherheit

Art. 7 DSG

Personendaten sind durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten zu schützen.

DSG & Datensicherheit: Massnahmen

Die Massnahmen müssen verhältnismässig sein.

Sie tragen folgenden Aspekten Rechnung:

- Zweck der Bearbeitung
- Art und Umfang der Bearbeitung
- Schätzung der möglichen Risiken für die betroffenen Personen
- gegenwärtiger Stand der Technik

Strafbestimmungen des DSG

Strafbar macht sich (auf Antrag):

- wer den Auskunfts-, Melde- und Mitwirkungs-pflichten vorsätzlich nicht, falsch oder unvollständig nachkommt,
- vorsätzlich eine falsche oder unvollständige Auskunft erteilt,
- wer vorsätzlich geheime, besonders schützenswerte Personendaten oder
- Persönlichkeitsprofile unbefugt bekannt gibt (Geheimhaltungspflicht).

Datenschutz

Zusammenfassung

- Vereinbarung und regelmässige Überprüfung der Sicherheitsmassnahmen mit Outsourcing-Partnern
- Vorsicht bei der Weitergabe oder Bekanntgabe von Daten an Dritte oder ins Ausland
- Erarbeitung und Kommunikation einer Privacy Policy
- Aufnahme der jeweiligen Verarbeitungen in die AGB's
- Speichern Sie keine besonders schützenswerten Informationen, wenn nicht unbedingt notwendig
- Bezeichnen Sie einen Datenschutzverantwortlichen, der ein Inventar der Datensammlungen führen muss

SWISS INFOSEC

Elektronische Archivierung

Einige ausgewählte Fragen

Rechtsbereiche

Allgemeine Anforderungen

- Historische Gründe
- Beweiszweck
  - Begründung von Ansprüchen
  - Unberechtigte Ansprüche abwehren

Forderungen durch den Gesetzgeber

- OR 957-962 (10 Jahre, Art. 958f OR)
  - Darstellung der Vermögenslage
  - Buchungsbelege (Rechnungen)
- BÜPF ?
  - Bundesgesetz betreffend Überwachung des Post- und Fernmeldeverkehrs
  - Eng auszulegen
- Spezialgesetze

Übersicht Revision GeBüV

Seit dem 1. Juni 2002

- Allg. Geschäftsbücher, Belege und Korrespondenz können in elektronischer Form geführt, bearbeitet, aufgezeichnet und aufbewahrt werden
- Bei der Aufzeichnung und Aufbewahrung von Geschäftsunterlagen sind die Grundsätze der ordnungsgemässen Buchführung einzuhalten
- Ordnungsgemäss aufgezeichnete und aufbewahrte elektronische Geschäftsunterlagen haben **die gleiche Beweiskraft wie ohne Hilfsmittel lesbare Dokumente**
- Elektronische Aufzeichnungen werden strafrechtlich als Urkunden anerkannt und geniessen dadurch rechtlich den Schutz gegen unerlaubten Zugriff, Zerstörung und Veränderung

Beweiskraft II

Mit der Revision ist der

Kreis der Unterlagen, die denselben Beweiswert wie Schrifturkunden haben, auf Dokumente ausgedehnt worden, die den Anforderungen der GeBüV bzw. der EIDI-V entsprechen.

Grundsatz der freien Beweiswürdigung

Beweiskraft

- Nachweis der ordnungsgemässen Aufzeichnung und Aufbewahrung
- Erhebungen über die Entstehung und die näheren Umstände der Aufzeichnung
- Wahrheitsgehalt der auf den Medien aufgezeichneten Informationen

Unklar ist Art der Eingabe des Beweismittels

- Sachverständigengutachten oder
- Eigene richterliche Infrastruktur

Pflicht zur Vorlegung von Originalen

- Entfällt, wenn Aufbewahrung auf Bild- und Datenträgern erlaubt ist
- keine nachteiligen Rechtsfolgen für eine Partei oder einen Dritten zulässig sind

Fazit:

Zur Stärkung des Beweiswertes muss vor Gericht die umfassende Einhaltung der einschlägigen Vorschriften, insbesondere GeBüV, aufgezeigt werden können, dies bedingt u.a. die umfassende Dokumentation der Verfahren und Prozesse.

Geschäftsbücherverordnung (GeBüV)

Ordnungsgemässe Datenverarbeitung

Neben einem Verweis auf die allgemeinen Grundsätze der ordnungsgemässen Buchführung, die in jedem Falle eingehalten werden müssen, bestimmt Art. 2 Abs. 2, dass bei elektronischer Führung und Aufbewahrung der Bücher, Belege und Geschäftskorrespondenz überdies die Grundsätze der ordnungsgemässen Datenverarbeitung zu beachten sind. Die Ordnungsmässigkeit der Führung und der Aufbewahrung der Bücher richtet sich gemäss Abs. 3 nach den allgemein anerkannten Regelwerken und Fachempfehlungen, sofern diese Verordnung oder darauf gestützte Erlasse keine Vorschrift enthalten

Geschäftsbücherverordnung (GeBüV)

Schutz Integrität

Archivierte Informationen müssen so erfasst und aufbewahrt werden, dass sie nicht geändert werden können, ohne dass sich dies feststellen lässt

Inventarisierung, Zugriff, Zutritt

Gemäss Art. 8 sind die Informationen systematisch zu inventarisieren und vor unbefugtem Zugriff zu schützen. Zugriffe und Zutritte sind aufzuzeichnen. Diese Aufzeichnungen unterliegen derselben Aufbewahrungspflicht wie die Datenträger.

Geschäftsbücherverordnung (GeBüV)

Schutz

Die archivierten Informationen sind sorgfältig, geordnet und vor schädlichen Einwirkungen geschützt aufzubewahren.
Die aufbewahrten Unterlagen müssen ausserdem jederzeit innert angemessener Frist eingesehen und geprüft werden können.

Trennung, Verantwortung

Archivierte Informationen sind von den aktuellen Informationen zu trennen bzw. so zu kennzeichnen, dass eine Unterscheidung möglich ist.
Die Verantwortung für die archivierten Informationen ist klar zu regeln und zu dokumentieren.

Geschäftsbücherverordnung (GeBüV)

Dokumentation

Die Organisation, die Zuständigkeiten, die Abläufe und Verfahren und die Infrastruktur (Maschinen und Programme), die bei der Archivierung zur Anwendung kommen, sind in Arbeitsanweisungen so zu dokumentieren, dass die Geschäftsbücher und die Buchungsbelege verstanden werden können.

Zur Stärkung des Beweiswertes muss vor Gericht die umfassende Einhaltung der einschlägigen Vorschriften, insbesondere GeBüV, aufgezeigt werden können, dies bedingt u.a. die hier dargestellte umfassende Dokumentation der Verfahren und Prozesse.

Detailbetrachtung E-Mail (I)

Motivation der E-Mail-Archivierung

- Technische Kapazitätsprobleme
  - Zunahme des externen und internen E-Mail Verkehrs (Tendenz steigend)
- Rechtliche Vorgaben
  - Gesetzliche Pflicht zur Archivierung, Probleme bei privaten Mails
  - Telefonnotizen, Interne Schriftstücke und E-Mails, sofern
    - für die interne Verwaltung eines Unternehmens oder Rechtsbeziehung mit Dritten von Bedeutung sind.
  - Regulatorische Verschärfung absehbar
  - Beweiskraft
    - Beweiskraft von ungeschützten Speicherungen (lokal/Server) und Papierausdrucken ist nicht gegeben, da nicht fälschungssicher
- Begründung von Rechten und Pflichten ist nach schweizerischem Recht an keine bestimmte Form, insbesondere nicht an die Schriftform gebunden (Art. 11 Abs. 1 OR), können mit E-Mails ohne weiteres rechtsverbindliche Erklärungen abgegeben werden, analog für Telefon

SWISS INFOSEC

Regeln der digitalen Forensik und ihre Grenzen

Was tun wenn es Probleme gibt?

Beweisrecht

- Beweisgegenstand
  - Zu beweisen sind Tatsachen (Zustände, Handlungen, Ursachen und Wirkungen), bei deren Verwirklichung die Rechtsfolge eintritt
- Beweislast
  - Die Beweislast für eine bestimmte Tatsache trägt derjenige, der aus dieser Tatsache für sich eine Rechtsfolge ableitet
- Recht auf Beweis
  - Es besteht Anspruch auf Abnahme von Beweisen, die dem Gericht zum Nachweis einer rechtserheblichen Tatsache frist- und formgerecht angeboten worden sind
- Beweismittel (Urkunden)
  - Schriften, die bestimmt und geeignet sind, oder Zeichen, die bestimmt sind, eine Tatsache von rechtlicher Bedeutung zu beweisen. Die Aufzeichnung auf Bild- und Datenträgern steht der Schriftform gleich, sofern sie demselben Zweck dient.

Beweisrechtliche Aspekte der Schweizerischen Strafprozessordnung

- Jede Person gilt bis zu ihrer rechtskräftigen Verurteilung als unschuldig.
- Das Gericht würdigt die Beweise frei nach seiner aus dem gesamten Verfahren gewonnenen Überzeugung. (Art. 10 StPO)
- Die Strafbehörden setzen zur Wahrheitsfindung alle nach dem Stand von Wissenschaft und Erfahrung geeigneten Beweismittel ein, die rechtlich zulässig sind. (Art. 139 StPO)
- Die Strafbehörden nehmen die Beweisgegenstände vollständig und im Original zu den Akten. Von Urkunden und weiteren Aufzeichnungen werden Kopien erstellt, wenn dies für die Zwecke des Verfahrens genügt. Die Kopien sind nötigenfalls zu beglaubigen. (Art. 192 StPO)
- Zwangsmassnahmen sind Verfahrenshandlungen der Strafbehörden, die in Grundrechte der Betroffenen eingreifen und die dazu dienen: Beweise zu sichern. (Art. 196 StPO)
- Zur Durchsetzung von Zwangsmassnahmen darf als äusserstes Mittel Gewalt angewendet werden; diese muss verhältnismässig sein. (Art. 200 StPO)

Ziele einer forensischen Untersuchung

- Definition
  IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.
  Leitfaden „IT-Forensik“, Version 1.0.1 (März 2011), BSI

- Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch geführt haben könnte
- Ermittlung des entstandenen Schadens nach einem Systemeinbruch
- Identifikation des Angreifers
- Sicherung der Beweise für weitere juristische Aktionen

Ziel der forensischen Untersuchung

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

Zusätzlich evtl. (Strafverfolgung, Sicherheitsbewertung)

- Wer hat es getan?
- Was kann gegen eine Wiederholung getan werden?

Methoden forensische Untersuchung

- Post-mortem-Analyse (Offline-Forensik)
  - Nachträgliche Aufklärung Vorfall
  - Untersuchung von Datenträgerabbildern («Images») auf nichtflüchtige Spuren
  - Gewinnung und Untersuchung von gelöschten, umbenannten sowie anderweitig versteckten und verschlüsselten Dateien von/auf Massenspeichern.
- Live-Forensik (Online-Forensik)
  - während Laufzeit des Vorfalls
  - Gewinnung und Untersuchung flüchtiger Daten
    - Hauptspeicherinhalt
    - Informationen über bestehende Netzwerkverbindungen
    - gestartete Prozesse.

Die Schritte einer forensischen Untersuchung

- Strategische Vorbereitung (mit was?)
- Operationale Vorbereitung (wie?)
- Datensammlung
- Datenuntersuchung
- Datenanalyse
- Dokumentation

Anforderungen forensische Untersuchung

- Akzeptanz
  - Methoden und Schritte in der Fachwelt beschrieben und akzeptiert
- Glaubwürdigkeit
  - Die Robustheit und Funktionalität der Methoden, ggfs. nachzuweisen
- Wiederholbarkeit
  - Hilfsmittel und Methoden müssen bei Wiederholung mit demselben Material dieselben Ergebnisse ergeben
- Integrität
  - Sichergestellte Spuren dürfen durch die Untersuchung nicht unbemerkt verändert worden sein. Die Sicherung der Integrität digitaler Beweise muss jederzeit belegbar sein.
- Ursache und Auswirkungen
  - Die Auswahl der Methoden muss logisch nachvollziehbare Verbindungen zwischen Ereignissen und Beweisspuren und evtl. Personen herstellen.
- Dokumentation
  - Jeder Schritt des Ermittlungsprozesses muss angemessen dokumentiert werden.

Anforderungen forensische Untersuchung - Dokumentation

- Die Authentizität der erhobenen Daten und des Vorgehens des Forensikers muss gewährleistet sein.
- Die Dokumentation muss die unternommenen Schritte innerhalb der gesamten forensischen Untersuchung (d.h. wer tat wann was) und daraus gewonnenen Resultate darlegen.
- Zusätzlich muss ein lückenloser Nachweises über den Verbleib von digitalen Spuren und der Ergebnisse der daran vorgenommenen Untersuchungen (engl. *Chain of custody*) erbracht werden.
- Es muss sichergestellt werden, dass zu jedem Zeitpunkt beginnend mit der Erfassung der digitalen Beweisspuren ein potentieller Missbrauch bzw. eine Verfälschung nachgewiesen werden kann.

Die Datensammlung

- Sammlung wichtiger Daten potentiell betroffener Komponenten
- Durchführung der Datensammlung ist zu dokumentieren
- Sammlung muss derart erfolgen, dass vollständige Erfassung und Speicherung erfolgt und keine Datenverfälschung vorkommt
- Dokumentation von Veränderungen bzw. unvollständigen Datensammlungen Erläuterung im Rahmen der abschliessenden Dokumentation
- Bewertung von Verfälschungsgrad und dessen Bedeutung beeinflusst Beweiskraft
- Datensammlung in der Reihenfolge ihrer Flüchtigkeit
- Forensisches Duplikat von allen betroffenen Massenspeichern
- Ablauf der Datengewinnung ist umfassend zu dokumentieren

Die forensische Duplikation eines Datenträgerabbildes (Image) 1/3

- Forensische Duplikation generell erforderlich
- Resultat ist 1:1-Kopie des Datenträgers, an welchem verschiedene Untersuchungsschritte mehrfach und ohne Veränderung der Originaldaten ausgeführt werden können
- Gibt auch Möglichkeit der Parallelisierung, d. h. mehrere Personen können denselben Datenträgerinhalt nach unterschiedlichen Gesichtspunkten und mit unterschiedlichen Methoden und Werkzeugen untersuchen
- Die Unverändertheit des Dateninhalts eines Datenträgers ist eine absolute Notwendigkeit, wenn dieser ein Beweisstück eines juristischen Prozesses ist

Die forensische Duplikation eines Datenträgerabbildes (Image) 2/3

Anforderungen an eine forensische Duplikation:

- *Physische Kopie* - Eine physische Kopie des Datenträgers ist herzustellen, d. h. der gesamte Sektorinhalt aller Sektoren des Datenträgers wird in die Datei hineingeschrieben
- *Fehlerbehandlung* - Lesefehler müssen eindeutig erkannt und protokolliert werden und durch vorher festgelegte Füllmuster ersetzt werden
- *Vollständigkeit des Abbildes* – Damit ein vollständiges Abbild erhalten wird, müssen reservierte Bereiche von Massenspeichern sicher erkannt und für den Zeitpunkt der Abbilderstellung deaktiviert werden
- *Unveränderthеit* - Die Erstellung des Abbildes muss mit der Berechnung einer kryptographischen Checksumme abgeschlossen werden, um die Unveränderthеit nachweisen zu können

Die forensische Duplikation eines Datenträgerabbildes (Image) 3/3

- Einsatz von Hardware-basierten Writeblockern zu Sicherstellung, dass auf betroffene Datenträger nur lesend zugegriffen werden kann
- Nur der Writeblocker-Einsatz, zwischen Datenträger und Schnittstelle des betroffenen Systems, unterbindet Schreibzugriff wirksam
- Nach Erstellung des Abbildes Berechnung einer kryptographischen Hashsumme über Originaldatenträger UND Image
- Übereinstimmende Checksummen belegen korrekte Ausführung der forensischen Duplikation und liefern so beweissichere Basis für die weiteren forensischen Untersuchungen

Die Benutzerweisung als Problemlöser

Obelix' Zaubertrank?

Schaffen Sie eine Win - Win - Situation !

Schaffen Sie Transparenz und Sicherheit

- Benutzungsweisung IT Mittel, unter Einschluss Internet und E-Mail
  - Erfüllung der gesetzlichen Vorgaben
  - Wahrnehmung der Sorgfalt seitens Management zum Schutz der unternehmenseigenen Informationen
  - Vereinbarung der Zugriffsrechte im Notfall und Verfahren
  - Schutz der Administratoren durch Festlegung der Rechte und Pflichten der IT-Abteilung und Administratoren
  - Klare Festlegung der Verfahren: Wer entscheidet auf wessen Antrag über welche Zugriffe und Datenempfänger
  - Darlegung sämtlicher Protokollierungen
  - Darlegung der Archivierungsregeln
- Einverständniserklärung des Mitarbeitenden notwendig
- ‚Jeder weiss, was Sache ist.'

Anforderungen seitens Arbeitgeber

Systemprotokollierung

- Wer hat was wann wo gemacht?
- Schutz der Systeme und der Reputation
- Legalisierung bereits bestehender Überwachungsmechanismen und Verdachtsmomente

Archivierung

Nachvollziehbarkeit

Zurechenbarkeit, Beweiskraft

Zugriff im Notfall

- Zugriff im Notfall (Krankheit, Ferien etc.) auf E-Mails des Arbeitnehmenden falls keine Stellvertreter-Regelung besteht
- Private Laufwerk des Arbeitnehmenden

Anforderungen (ohne «Deal »)

Privatsphäre des Arbeitnehmers

- Wahrung des Briefgeheimnisses
- Achtung persönlicher Sachen
- Keine systematische Leistungskontrolle
- Kein Zugriff auf private E-Mails und keine personenbezogene Auswertung des „Surfens“
- Personenbezogene Protokollierung nur zulässig basierend auf **Überwachungsreglement und „Vorwarnung“**
- Schutz der Privatsphäre
  - Protokollierung der privaten Kommunikation ist i.d.R. unzulässig
  - Protokollierung der geschäftlichen Kommunikation ist bei Vorliegen eines Rechtfertigungsgrundes zulässig (Art. 13 DSG)

Zulässige Protokollierung durch Arbeitgeber

(ohne «Deal»)

- **Rechtfertigungsgründe**
  - Nur zum Schutz und Leistungskontrolle der Mitarbeiter, sofern vorherige Zustimmung und Eingriff verhältnismässig. Keine Verhaltenskontrolle (Art. 26 V 3 ARG)! Zeitlich beschränkt. Keine Beurteilung einzig gestützt auf die Kontrolle.
- **Einblick in private Daten durch Arbeitgeber: unzulässig**
  - Sofern nicht zwischen geschäftlicher und privater Kommunikation unterschieden wird, ist der höhere Schutzstandard zu beachten!
- **Archivierung der privaten Mails während 10 Jahren ist unverhältnismässig**
- **Nichteinhaltung der gesetzlichen Vorgaben und Regelungen kann als widerrechtliche Persönlichkeitsverletzung (Art. 15 und 25 DSG) gerichtlich beurteilt werden**
- **Aus Missbrauch resultierende Sanktionen sind ebenfalls anfechtbar (z.B. missbräuchliche Kündigung nach Art. 336 OR)**

Monitoring / Logging im Arbeitsverhältnis

Auswertung von Protokolldaten im Arbeitsverhältnis (1/3)

- Gestattet sind **permanente anonymisierte** Auswertungen der Protokollierungen sowie **stichprobenartige pseudonymisierte** Auswertungen der Protokollierungen, um zu überprüfen, ob das Nutzungsreglement eingehalten wird
- Die Überwachung der Auswertungen der Internetprotokollierungen unterteilt sich in zwei Phasen:
  - **Nichtpersonenbezogene** Überwachung;
  - **Personenbezogene** Überwachung.

Monitoring / Logging im Arbeitsverhältnis

Auswertung von Protokolldaten im Arbeitsverhältnis (2/3)

- **Grundsatz:** Statt die Arbeitnehmer zu überwachen sollen technische Schutzmassnahmen gesetzt, die unerwünschtes Surfen in Grenzen halten und das Unternehmen vor technischem Schaden schützen. Nur wenn ein Missbrauch so nicht verhindert werden kann, dürfen nach Erlass eines Nutzungsreglementes und nach **vorheriger Information im Einzelfall personenbezogene Auswertungen der Protokollierungen** vorgenommen werden.
- Fehlt ein Missbrauch und eine vorherige Information, dürfen die Internet- und E-Mail-Protokollierungen nur in **anonymer oder pseudonymer** Weise ausgewertet werden.

Monitoring / Logging im Arbeitsverhältnis

Auswertung von Protokolldaten im Arbeitsverhältnis (3/3)

- Ob Protokollierungen eingesetzt werden dürfen, wer und wie lange darauf Zugriff hat, muss nach den Kriterien der **Zweck-** und **Verhältnismässigkeit** entschieden werden. Ein Hinweis auf jede eingesetzte Protokollierung, deren Zweck, Inhalt und Aufbewahrungsdauer sollte aus Transparenzgründen im internen Überwachungsreglement erwähnt werden.
- Wenn **präventive Massnahmen** den Schutz sensibler Personendaten nicht gewährleisten, können Protokollierungen notwendig sein (Art. 10 Verordnung zum Datenschutzgesetz, VDSG, SR 235.11).

Inhalt Acceptable Use Policy

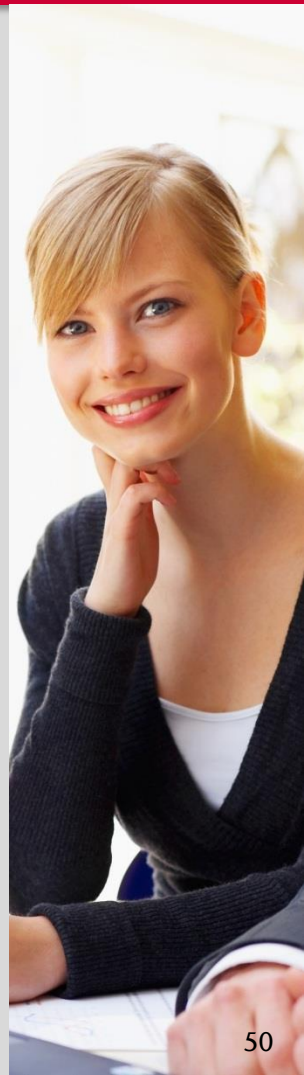
AUP

- Information, dass Auswertungen stattfinden.
- Information, dass personenbezogene, teilweise automatisierte Auswertungen stattfinden.
  - Somit werden auch intensivere Inhouse-Ermittlungen ermöglicht und legalisiert
- Einverständnis des Mitarbeitenden

Wichtige Anmerkungen

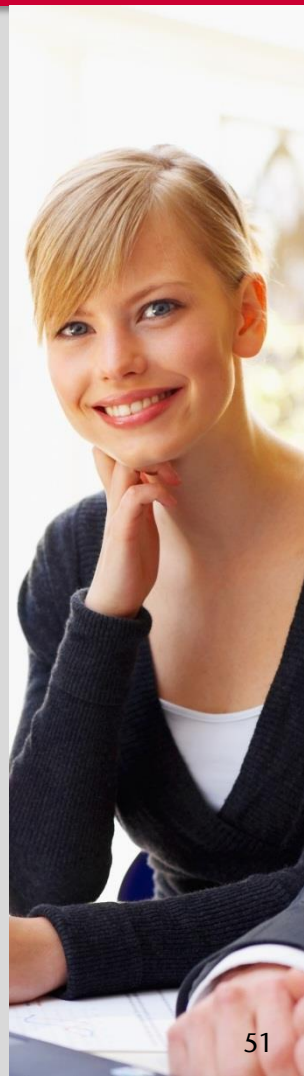
!!!

- **Mitarbeitende müssen schriftlich ihr Einverständnis geben**
  - Beweiszeck
  - Achtung: Einverständniserklärung könnte widerrufen werden
- **Mitarbeitende können Löschung privater Daten verlangen**
  - Sofern für die Abwicklung des Arbeitsvertrages nicht benötigt
  - E Mail Archivierung!
  - Sollten private oder als privat markierte E-Mails der Mitarbeitenden archiviert worden sein, haben die MA das Recht, diese löschen zu lassen (selbst einzelne E-Mails)
- **Mitarbeitende nehmen «Deal» sehr positiv auf, sofern spürbar, dass Management seinerseits hinter den definierten Regeln steht, diese vorlebt und selber auch einhält**



Resultat

- ✓ Privatsphäre der Mitarbeiter ist geschützt
- ✓ Unternehmensinteressen bleiben gewahrt
- ✓ Handelnde Personen kennen ihre Rechte und Pflichten und verstossen nicht gegen Gesetze oder die Rechte der Betroffenen
- ✓ Die Rechte und Pflichten aller Mitarbeitenden bezüglich Umgang mit IT Mitteln sind klar definiert.



SWISS **INFOSEC**

VIELEN DANK

Ihre Lösung beginnt mit einem Kontakt bei uns: +41 41 984 12 12, infosec@infosec.ch

reto.zbinden@infosec.ch | +41 (0)79 446 83 00

25 years
security@its best
www.infosec.ch

Consulting
Supporting
Training

Zürich
Bern
Sursee

Integrale Sicherheit
Informationssicherheit
IT-Sicherheit
Datenschutz