DER INNOVATION
DEN WEG BEREITEN ...

STAHL COMPUTERTECHNIK

Datenschutzfrühstück

dD datenschutz Daubmeier

datenschutz Daubmeier

Datenschutz- und IT Beratung

MOOSBURGER HOF

Fabian Stahl

26.06.2017

DAS UNTERNEHMEN – FAKTEN & ZAHLEN

STAHL COMPUTERTECHNIK

- seit Juli 2005 erfolgreich am Markt
- 19 Mitarbeiter mit 7/24 Hotline auf Wunsch
- Büro in der Pfaffenhofener Innenstadt am Hauptplatz
- unabhängiger IT-Dienstleister
- statten klein- und mittelständische Unternehmen in der Region um Pfaffenhofen, aber auch überregional umfassend mit IT-Infrastruktur, Kommunikationstechnik und Telekommunikation aus

DAS UNTERNEHMEN – ANGEBOT

STAHL COMPUTERTECHNIK

IT-SERVICE
Alles rund um Server, Clients & Netzwerk

KOMMUNIKATION
Telefonanlagen & Datenkommunikation

CLOUD-SERVICES
Exklusive Lösungen aus Cloud und Rechenzentrum

SOFTWARE
Standardsoftware & Programmierung

IT-SYSTEMPARTNER FÜR UNTERNEHMEN

STAHL COMPUTERTECHNIK

DATENSCHUTZ BEI STAHL

STAHL COMPUTERTECHNIK

Herbst 2014
Schulung eines eigenen MA´s für Datenschutz inkl. Zertifizierung (es durfte kein MA sein der in Verwaltung, Vertrieb und Technik tätig ist)

Februar 2015:
Beginn der strukturierten und durchgängigen Umsetzung des Datenschutz mit externem DSB

Juli 2015:
Auslieferung der ersten überarbeiteten Auftragsdatenverarbeitungsverträge an unsere Kunden

erstmalig im Februar 2016:
Unterstützung von Unternehmen bei der ISO Zertifizierung

laufendes Jahr 2016
Beschreiben der TOM´s bei den eigenen vWORK Produkten

laufende Betreuung
Information des DSB über Gesetzesänderungen, Aktualisierungen der bestehenden Dokumente, mind. 1 jährlich Datenschutzunterweisung der Mitarbeiter/innen

bis Januar 2018 geplant
Aktualisieren aller Dokumente für die Datenschutz Grundverordnung die ab 2018 gelten wird

UNSER REFERENT HEUTE

STAHL COMPUTERTECHNIK

Hubert Daubmeier

DER INNOVATION
DEN WEG BEREITEN ...

STAHL
COMPUTERTECHNIK

Stahl Computertechnik GmbH
Hauptplatz 11 · 85276 Pfaffenhofen a. d. Ilm
T +49 8441 40858-0
info@stahlgmbh.de

Datenschutz-Frühstück
Hotel Moosburger Hof
26. Juni 2017

Worüber wir heute sprechen

1. Kurze Einführung in den Datenschutz
2. Verpflichtung auf das Datengeheimnis
3. Datenschutzerklärung auf Ihrer Web Site
4. Nutzung von Firmenhandys
5. Private E-Mail und Internetnutzung am Arbeitsplatz
6. Was kommt mit der Datenschutz Grundverordnung

Bitte melden Sie sich gleich bei Fragen

Diese Unterlage finden Sie auf https://daubmeier.de

GRUNDBEGRIFFE

Personenbezogene Daten

- Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.

  Typische Beispiele für personenbezogene Daten
  - Informationen zur Person (Name, Aussehen)
  - Adresse und Kommunikationsdaten (Anschrift, Telefon-Nr., E-Mail-Adresse)
  - Bankverbindungs-/ Kreditkartendaten
  - Identifikationsmerkmale (Ausweisnummern, Kfz-Kennzeichen

Personenbezogene Daten

Wichtig bei personenbezogenen Daten

- Personenbezug muss nicht immer direkt herstellbar sein, damit Daten als personenbezogene Daten gelten.

  Beispiel: IP-Adressen, Kfz-Kennzeichen

- Bezug muss zu einer natürlichen Person bestehen, juristische Personen haben grundsätzlich keine sie betreffenden personenbezogenen Daten.

Personenbezogene Daten

Besondere Arten personenbezogener Daten

- Sind wegen ihrer Sensibilität besonders schützenswert.

  Das heißt für das Erheben, Verarbeiten und Nutzen gelten verschärfte Rahmenbedingungen.

- Besondere Arten personenbezogener Daten sind Angaben über:
  - die rassische und ethnische Herkunft,
  - politische Meinungen,
  - religiöse oder philosophische Überzeugungen,
  - Gewerkschaftsmitgliedschaft

Erheben, Verarbeiten, Nutzen

- Erheben ist das Beschaffen von Daten über den Betroffenen.
- Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.
- Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

GRUNDPRINZIPIEN

Grundprinzipien im Datenschutz

Erlaubnisvorbehaltsprinzip

- Das Erheben, Verarbeiten oder Nutzen personenbezogener Daten unterliegt dem Erlaubnisvorbehalt.
- Das Erheben, Verarbeiten oder Nutzen ist gemäß § 4 Abs. 1 BDSG nur zulässig, wenn
  - das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet

  Oder

  - die Einwilligung des Betroffenen vorliegt.

Fehlt die Rechtsgrundlage, müssen vorhandene Daten wieder gelöscht werden.

Grundprinzipien im Datenschutz

Transparenz

- Der Umgang mit personenbezogenen Daten darf nicht heimlich erfolgen.
- Es muss für eine betroffene Person transparent, das heißt erkennbar und nachvollziehbar sein,
  - wer
  - welche personenbezogenen Daten
  - für welchen Zweck
  - in welcher Weise

  erhebt, verarbeitet oder nutzt.

Grundprinzipien im Datenschutz

Datensparsamkeit und Datenvermeidung

Das Minimalprinzip ist in § 3a BDSG verankert:

- Erheben, Verarbeiten und Nutzen personenbezogener Daten und
- Auswahl und Gestaltung von Datenverarbeitungsverfahren
- müssen sich am Ziel orientieren, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.
  - Beispiel: Bei einem Bestellformular sind nur Name, Anschrift, Bankverbindung, E-Mail-Adresse Pflichtfelder; andere Angaben (z. B. Geburtsdatum) sind freiwillig.

Grundprinzipien im Datenschutz

Zweckbindung

- Schon vor der Erhebung von Daten muss der Zweck der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten festgelegt sein.

- Nur für den festgelegten Zweck dürfen Daten verarbeitet oder genutzt werden.

Grundprinzipien im Datenschutz

Erforderlichkeit

- Beim Erheben, Verarbeiten oder Nutzen personenbezogener Daten ist immer danach zu fragen, ob dies für die Erreichung des Zwecks erforderlich ist.
- Erforderlichkeit bedeutet in der Regel auch
  - Prüfung der Verhältnismäßigkeit, das heißt ist etwa ein bestimmtes Erheben, Verarbeiten oder Nutzen geeignet, erforderlich und angemessen.
  - Abwägung zwischen berechtigten Interessen der verantwortlichen Stelle und der schutzwürdigen Interessen der Betroffenen.

Grundprinzipien im Datenschutz

Einwilligung

Einwilligung ist die vorherige Zustimmung	Genehmigung ist die nachträgliche Zustimmung
Im Datenschutzrecht gibt es nur die Einwilligung!	

- Das nachträgliche Einholen einer Einwilligung (= eine Genehmigung) macht ein Erheben, Verarbeiten oder Nutzen personenbezogener Daten nicht im Nachhinein zulässig.

- Einwilligung im Datenschutz gilt nicht für immer und ewig! Sie kann für die Zukunft widerrufen werden.

Grundprinzipien im Datenschutz

Typische Probleme bei der Einwilligung

- Meist die Schriftform erforderlich. Elektronisch oft möglich
- „Verstecken“ im Kleingedruckten
- freie Willensentscheidung
- Information über den Verwendungszweck und Datenweitergabe
- Einwilligung durch Minderjährige
- Einwilligung bei Marketing und Werbung
- Einwilligung bei besonderer Arten personenbezogener Daten

  Beispiel: Gesundheitsdaten sollen bei betrieblichen Wiedereingliederungsmaßnahmen erhoben, verarbeitet, genutzt werden → spezielle Einwilligung erforderlich

DATENGEHEIMNIS

Was sagt das BDSG?

Bundesdatenschutzgesetz

Erster Abschnitt - Allgemeine und gemeinsame Bestimmungen (§§ 1 - 11)

§ 5
Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Datengeheimnis – wie umsetzen?

Vorlage vom Bayerischen Landesamt für Datenschutzaufsicht laden und anpassen

- www.lda.bayern.de – suche „Datengeheimnis“
- Auf eigenen Betrieb anpassen, z.B. Kopfzeile. Und zukunftsfest machen. Mögliche Formulierung:
  … gemäß § 5 BDSG bis 24.5.2018 und ab 25.5.2018 nach den allgemeinen Grundsätzen der EU Datenschutzgrundverordnung 2016/679.
- Unterschriebene Verpflichtungserklärung in der Personalakte ablegen
- Merkblatt verbleibt beim Mitarbeiter

DATENSCHUTZERKLÄRUNG AUF IHRER WEBSEITE

Einladung für Abmahner

§ 5 Telemediengesetz (TMG) ist hinlänglich bekannt

§ 13 Abs 1, Satz 1 TMG bestimmt, dass ein Nutzer eines Telemediums (darunter fallen auch private Homepages), "zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten [...] zu unterrichten ist".

- Laut Satz 3: "Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.„

Angebot

Die Umsetzung der Datenschutzerklärung erfordert

- die rechtliche Seite
- die technische Seite

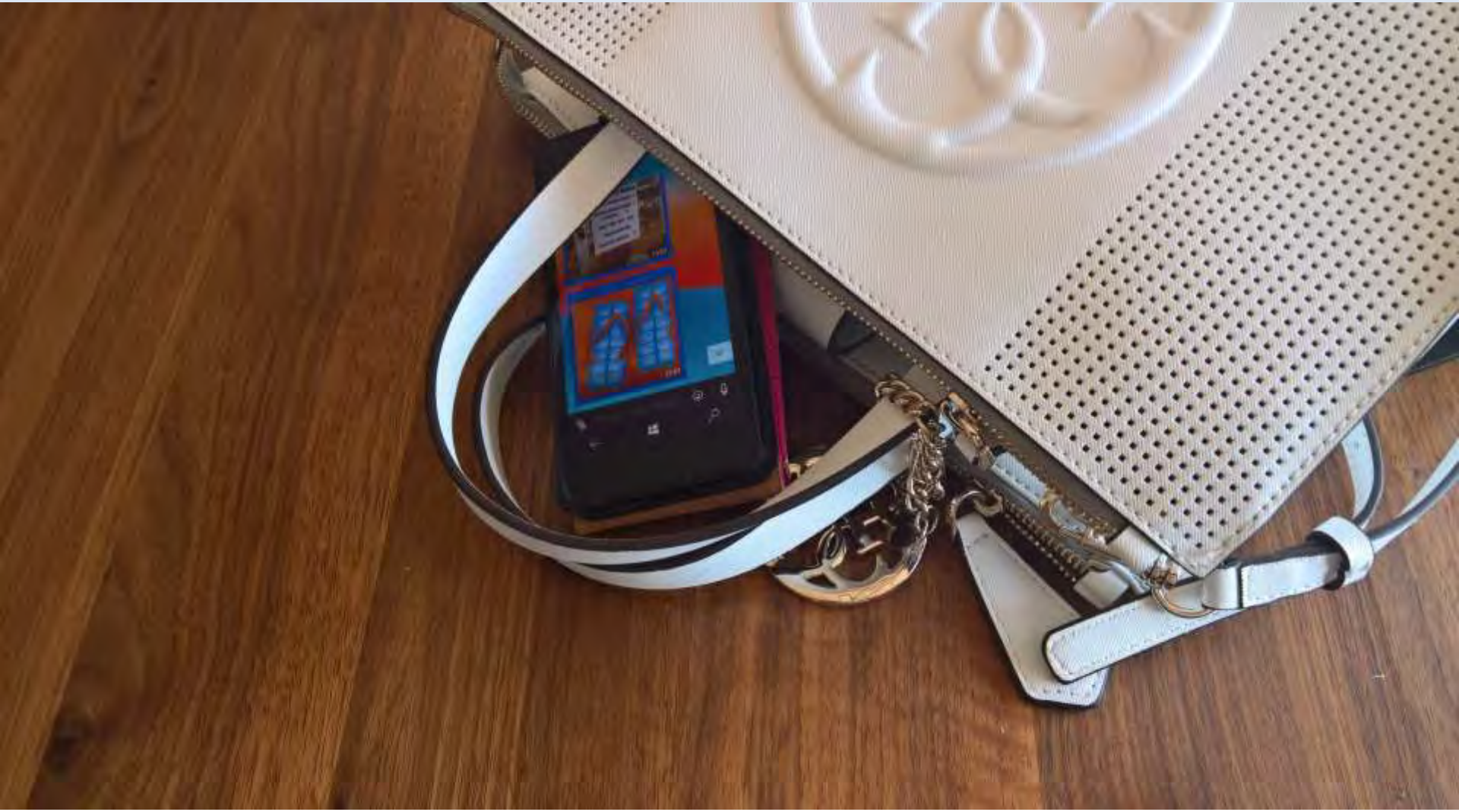
Sonderangebot zum Datenschutzfrühstück von Stahl Computer und datenschutz Daubmeier

- Wir kümmern uns um beides
- zum günstigen Festpreis

Bitte sprechen Sie uns an

NUTZUNG VON FIRMENHANDYS

„Bring your own desaster“?



So kann es gehen

a) Arbeitgeber stellt Smartphone und trägt Gebühren
b) Datenschutzanforderungen einhalten
c) Interne Nutzungsregeln
d) Technische Expertise
e) Sonstiges

Datenschutz Grundannahme

- Es fallen personenbezogene Daten an
  (andernfalls würden Einfachmobiltelefone ausreichen)
  - Kontaktdaten, Gesprächsdaten
  - Fotos und Filme
  - Emails, Nachrichten / SMS, Messages / Whatsapp
  - Dokumente
  - Standortdaten (GPS)
  - Gerätedaten (IMEI, MAC Adresse, Konto)
  - Apps (Kauf direkt, InApp Käufe, Fremdstore)
  - Browserdaten (Verlauf, Cookies, …)
  - Biometrische Daten (Fingerabdruck, Irisscan)

Datenschutz Grundannahmen fortges.

- Verlust oder Diebstahl von Geräten muss die Grundannahme sein und nicht die unvorhersehbare Ausnahme.
  - Verschlüsseln - Gerät
  - Verschlüsseln - Speicher
  - Verschlüsseln – Dateien mit besonderen Arten personenbezogener Daten
- Sicherungsmaßnahmen werden von technisch versiertem Personal erbracht
  - Einsatz MDM
  - Prüfung zugelassener Apps
  - Kontrolle des Einsatzes
  - Update und ggf. Zurücksetzen des Geräts

Datenschutzkonfiguration

- Trennung von privaten und dienstlichen Daten. Bzw. entsprechende Regelung.
  - Bei Verbot besteht Kontrollpflicht durch Arbeitgeber.
  - Bei Erlaubnis kein Zugriff auf private Daten durch AG.
- Besondere Arten von personenbezogenen Daten sind per Dateiverschlüsselung, zu sichern
- Keine personenbezogenen Daten in der Cloud. Nur verschlüsselte Daten (Dateikennwort oder z.B. BoxCryptor)

Technische Konfiguration

- Updates zeitnah einspielen. Regelung durch wen dies erfolgen soll.
- Aktueller Virenschutz (wenn möglich)
- Geräte sind verschlüsselt und mit Anmeldekennwort oder PIN Code gesichert.
- Keine unsicheren biometrische Verfahren zur Anmeldung
- Der Benutzer im Geräte-Store sollte der Arbeitgeber sein.
- Zurücksetzen des Geräts nur durch Beauftragte.
- Abgabe der Geräte an Kinder (etwa zum Spielen) und Dritte untersagen., falls keine technischen Vorkehrungen dafür existieren
- Emailverkehr über verschlüsselte Übertragungsprotokolle.
  D.h. Clients richtig konfigurieren.

Organisatorische Empfehlungen

- Definierter Prozess und zeitnahe Reaktion bei Verlust und Diebstahl
- Regelung von Nutzungskosten und erlaubtem Datenvolumen.
- Arbeitsverträge prüfen ggf. anpassen

Sonstige Erfordernisse

- Zustimmung des Betriebsrats erforderlich (§ 87 Abs. 1 Nr. 6 BetrVG)
- Einhaltung von Aufbewahrungspflichten, etwa nach § 257, Abs. 1 HGB und § 147 AO. beachten
- Einhaltung der geltenden Arbeitszeitregelungen (u.a. § 3 ArbZG und § 10 Abs. 1 ArbZG - Einsatz von Smartphones an Sonn- und Feiertagen)
- Keine Leistungs- und Verhaltenskontrollen!
- Beachten von Geheimhaltungsverpflichtungen Kunden gegenüber

Nutzungsregeln

- Kein Zwang zur Nutzung. Einwilligung einholen.
- Regelung der privaten Nutzung von Email und Internet (siehe dort)
- Verbot des Arbeitgebers auf private Daten zuzugreifen.
- Urheberrechte der genutzten Software beachten
- Kein Datenaustausch mit privaten Geräten, z.B. Drucker, Privat-PC
- Modding / Jailbreak / Rooting untersagen
- Kein Abschluss von Rechtsgeschäften über Smartphone, da damit Archivierungspflichten entstehen könnten.
- Schulung der Mitarbeiter in die Bedienung des Geräts. Inkl. Privacy Settings u. Policy
- Herausgabe des Geräts bei Beendigung des Arbeitsverhältnisses

PRIVATE E-MAIL UND INTERNET-NUTZUNG AM ARBEITSPLATZ

Rechtsgrundlagen

- Fernmeldegeheimnis, § 88 Abs. 2 S. 1 TKG
- Besondere Zweckbindung u.a. § 31 BDSG
- Datenerhebung, § 11 Abs. 1 Nr. 1 TMG
- Verletzung des Fernmeldegeheimnisses § 206 StGB
- Aufbewahrungspflichten u.a. § 147 AO und weitere aus dem HGB, GoBD.

Greift das Fernmeldegeheimnis?

- Nach Ansicht der Aufsichtsbehörden (AB) im Düsseldorfer Kreis: ja.
  - Zahlreiche Veröffentlichungen dazu
- Nach Ansicht einiger Gerichte: nein
  - Kommt auf den Einzelfall an. Urteile sind zu prüfen
- Betroffene können sich leicht(er) und einfach(er) an die Aufsichtsbehörden wenden
  - Solange keine höchstrichterliche Entscheidung vorliegt die einzig praktikable Interpretation.

Hinweis: der „ruhende“ E-Mail-Verkehr steht dem „dynamischen“ Telekommunikationsvorgang gleich

Haben wir personenbezogene Daten?

Rechte des Arbeitgeber – allgemein

- Grundsatz

  Soweit der Arbeitgeber Hardware bzw. Software zur Verfügung stellt, dürfen die betrieblichen Internet- und E-Mail-Dienste grundsätzlich nur für die betriebliche Tätigkeit genutzt werden.

- Dem Arbeitgeber steht es frei, ob er eine Privatnutzung des Internets und/oder des betrieblichen E-Mail-Accounts erlaubt.

- Bei Kenntnis und Duldung der privaten Nutzung über einen längeren Zeitraum (sog. „betriebliche Übung“) gilt die private Nutzung als konkludent genehmigt.

Optionen für den Arbeitgeber / Betrieb

a. Private Nutzung von Internet und E-Mail erlaubt
b. Private Nutzung von Internet und E-Mail verboten
c. Private Nutzung von Internet erlaubt und E-Mail verboten
   - Hinweis auf Nutzung privater web-basierter Dienste

Aber dringende Empfehlung die private Nutzung zu regeln und die Einwilligung der Mitarbeiter einholen für die Vertretungsregelung.

Vergleichstabelle

	Email erlaubt Internet erlaubt	Email verboten Internet verboten	Email verboten Internet erlaubt
Bestimmendes Gesetz	TMG	BDSG	BDSG
Zugriff durch AG	Mit Einwilligung	Möglich (nicht private)	Möglich (nicht private)
Einwilligung AN	Zwingend erforderlich	Nicht erforderlich	Empfohlen
Vertretungsregelung	Erforderlich	Empfohlen	Empfohlen
Logdaten	Bestimmungsgemäß	Bestimmungsgemäß *	Bestimmungsgemäß
Verhaltens- und Leistungskontrolle	Nicht erlaubt	Nicht erlaubt *	Nicht erlaubt
Kontrollpflicht	Nein	Ja *	Nein
Geheimnisträger	Kein Zugriff	Kein Zugriff	Kein Zugriff
Kontolöschung (E-Mail)	Umgehend bei Beendigung	Aktiv solange erforderlich	Nicht zutreffend
Archivierung	Schwierig	Möglich	Möglich

Vergleich im Detail

- Zugriff auf betriebliche E-Mails (mit Einwilligung oder weil Privatnutzung verboten)
  - Einzelne oder fest definierte E-Mails einzeln zur Kenntnis zuleiten.
  - Keine automatisierte Weiterleitung aller ein- und ausgehenden Emails
  - Verbot der permanenten Kontrolle

- Weiterleitung der E-Mails bei Abwesenheit
  - PN verboten: Abwesenheitsassistenten sollte vorgezogen werden, da schutzwürdige Belange der Beschäftigten zu beachten sind.
  - PN erlaubt: interne betriebliche Lösung anstreben (nicht jeder Beschäftige muss/wird Einwilligung erteilen).
  - Ungeplante Abwesenheit berücksichtigen.

- Private E-Mails dürfen von dem Arbeitgeber nicht weiter inhaltlich zur Kenntnis genommen werden, sobald ihr privater Charakter erkannt wurde (beide Fälle - auch bei Verbot gibt es private E-Mails)
  - Ausnahme Missbrauchskontrolle.

Vergleich im Detail II

- Kontrolle der Internet-Nutzung
  - Privatnutzung erlaubt: AG darf Nutzung kontrollieren
  - Privatnutzung verboten: AG **muss** Nutzung kontrollieren
  - In beiden Fällen gilt stichprobenartig und ohne Identifizierung der einzelnen Beschäftigten
- Bei Aufdeckung von Straftaten (beide Fälle)
  - tatsächliche Anhaltspunkte
  - muss zur Aufdeckung erforderlich sein
- Datenschutzkontrolle, Datensicherung oder Sicherung des ordnungsgemäßen Betriebs
  - Keine Verhaltens- und Leistungskontrolle der Beschäftigten

Zusammenfassend

1. Betriebsinterne Regelung der privaten Internet- und E-Mail Nutzung dringend empfohlen

2. Personenbezogene Vollkontrolle ist ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung der Beschäftigten

RECHTE DES BETROFFENEN

Rechte des Betroffenen

Recht auf Auskunft

- Verlangt ein Betroffener Auskunft, muss die verantwortliche Stelle grundsätzlich Auskunft geben über
  - die zu seiner Person gespeicherten Daten,
  - den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden und
  - den Zweck der Speicherung.
- Auskunftsrecht besteht unabhängig von einer Rechtsbeziehung zwischen verantwortlicher Stelle und Betroffenem, das heißt er muss nicht beispielsweise Beschäftigter oder Kunde sein.

selbstauskunft.net

TFFFF oder T5F

Sehr geehrte Damen und Herren,

Gemäß Bundesdatenschutzgesetz (BDSG) fordere ich Sie auf:

mir gegenüber unverzüglich offenzulegen, welche Daten Sie über mich gespeichert haben, und aus welchen Quellen sämtliche mich betreffenden Daten stammen.

- Sie haben den Verwendungszweck sämtlicher mich betreffenden Daten unverzüglich mir gegenüber offenzulegen.
  Sie haben sämtliche meine Person betreffenden Daten unverzüglich zu sperren und mir diese Sperrung zu bestätigen.
- Ich untersage Ihnen jedwede zukünftige Speicherung meine Person bzw. meine Adressen betreffenden Daten ohne meine vorherige ausdrückliche schriftliche Genehmigung.
- Ich untersage Ihnen die Übermittlung dieser Daten an Dritte. Für bereits übermittelte Daten fordere ich eine unverzügliche Sperrung.
- Ich setze Ihnen zur Erfüllung dieser Forderung eine Frist von zwei Wochen.

Bitte haben Sie Verständnis dafür, dass - sollten Sie dieses Schreiben ignorieren - mich gezwungen sehe, den zuständigen Landesdatenschutzbeauftragten zu informieren.

Ich bedanke mich im Voraus für Ihre Kooperation.

Mit freundlichen Grüßen

Google.de meldet „Ungefähr 1300 Ergebnisse“ auf den obigen Suchbegriff

Rechte des Betroffenen

Recht auf Berichtigung

– Personenbezogene Daten müssen berichtigt werden, wenn sie unrichtig sind.

Beispiel:

- Ein Betroffener stellt fest, dass von seiner Bank eine falsche Kredithöhe bei der Schufa gemeldet wurde. Die unrichtige Information muss berichtigt werden, da dies Auswirkungen auf die Kreditwürdigkeit (Scorewert) haben kann.

Rechte des Betroffenen

Recht auf Löschung oder Sperrung

Personenbezogene Daten müssen insbesondere dann gelöscht werden, wenn

- die Speicherung an sich schon unzulässig ist (z. B. bei fehlender Rechtsgrundlage) oder
- deren Kenntnis für den mit der Speicherung verfolgten Zweck nicht mehr erforderlich ist (z. B. Löschung der Adressdaten nach Abschluss eines Preisausschreibens).

Wichtig: Bestehen Aufbewahrungspflichten oder stellt das Löschen einen unverhältnismäßig hohen Aufwand dar, muss anstatt gelöscht gesperrt werden.

ÜBERBLICK ZUR EU DATENSCHUTZ GRUNDVERORDNUNG (DS-GVO)

EU Datenschutzgrundverordnung

EU-Amtsblatt vom 4.5.2016, L 119/1 ff.

- Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), VO 2016/679

25.06.2017	
25.05.2018	
334	Tage
- 96	Samstage und Sonntage
- 30	Urlaubstage
- 11	Feiertage
- 5	Krankheitstage
- 3	Sonstige Ausfalltage
189	**Arbeitstage**

Reformziele im Überblick

- Digitaler Binnenmarkt
- „Goldstandard“ für den Datenschutz in einer vernetzten Welt
- Modernisierung und Rechtsvereinheitlichung
- Ergänzung der rechtlichen durch tatsächliche Kohärenz
- Stärkung der Eigenverantwortung („Accountability“), der Betroffenenrechte und der der Datenschutzbehörden
- Stufenkonzept, keine Gesamtreform

Auswirkungen auf das deutsche Datenschutzrecht

Anwendungsvorrang einer EU-Verordnung
- umfassende und unmittelbare Verbindlichkeit
- beansprucht Anwendungsvorrang gegenüber nationalem Recht
  - Nicht einmal Wiederholen der Regelungen oder Definitionen der DS-GVO
- Ziel: Harmonisierung

- Spielräume für nationales Recht
  - Öffnungsklauseln („Kann-Regelung)
  - Regelungsaufträge („Muss-Regelung“)

- Führt zu umfassenden Rechtsbereinigungsaufgaben
  - Bundestagswahlen im Herbst 2017

Was bedeutet dies für uns?

Ausgesuchte Änderungen

a. Datenpannen
b. Kleiner Satz mit großer Wirkung
c. Datenschutzfolgenabschätzung
d. Geänderte Rolle der Aufsichtsbehörden

Umgang mit Datenpannen

Artikel 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

- …

…es sei

…rt …

Zukün…

- Jede…
- Jede… unver…
- Jeder … (soferr…
- Jeder H…
- Jeder D…

…die Überprüfung …haltung der Bestimmungen dieses Artikels ermöglichen.

Erfolgt die Meldung an die Aufsichtsbehörde nicht bzw. nicht innerhalb von 72 Stunden oder ohne Begründung bei Verzögerung, so besteht der neue Bußgeldrahmen (10 Mio. Euro bzw. 2% des Umsatzes)

Neu: die Aufsichtsbehörde hat keinen Ermessensspielraum mehr. Sie muss sanktionieren.

Aktuelles vom BayLDA

Datenpannen: Vergleich heute & morgen

	BDSG	DS-GVO
Meldung an die Aufsichtsbehörde BayLDA	§ 42a BDSG Nur wenn sensible Daten betroffen sind und schwerwiegende Beeinträchtigungen drohen	Art. 33 DS-GVO Bei jedem Vorfall, unabhängig von der Art der personenbezogenen Daten, es sei denn, es besteht voraussichtlich kein Risiko
Benachrichtigung des Betroffenen 	§ 42a BDSG Nur wenn sensible Daten betroffen sind und schwerwiegende Beeinträchtigungen drohen	Art. 34 DS-GVO Nur wenn ein hohes Risiko für den Betroffenen besteht und der Verantwortliche das Risiko nicht eliminiert hat

Kleiner Satz mit großer Wirkung

Art 5 - Grundsätze für die Verarbeitung personenbezogener Daten

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Was muss eingehalten und nachgewiesen werden?

- Transparenz der Verarbeitung für den Betroffenen
- Zweckbindung der Verarbeitung
- Grundsatz der Datenminimierung
- Richtigkeit der personenbezogenen Daten
- Löschen und Sperren von Daten
- Schutz vor unbefugten Zugriffen/Änderungen

Datenschutzfolgenabschätzung

Artikel 35 - Datenschutz-Folgenabschätzung

(1) … Verarbeitung, insbesondere bei Verwendung neuer Technologien, … voraussichtlich ein hohes Risiko für die Rechte und Freiheiten … so führt der Verantwortliche vorab eine Abschätzung der Folgen … durch..

3) … insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte … einschließlich Profiling …

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten …

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Inhalt der Folgenabschätzung

Artikel 35 - Datenschutz-Folgenabschätzung

(7) Die Folgenabschätzung enthält zumindest Folgendes:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge
- eine systematische Beschreibung der Zwecke der Verarbeitung,
- gegebenenfalls … der … verfolgten berechtigten Interessen
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit … in Bezug auf den Zweck
- eine Bewertung der Risiken …
- die zur Bewältigung der Risiken geplanten
  - Abhilfemaßnahmen,
  - Garantien,
  - Sicherheitsvorkehrungen
  - Verfahren, durch die der Schutz personenbezogener Daten sichergestellt
- der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird

Neue Interaktion mit Aufsichtsbehörden

- Der Name und Kontaktdaten des Datenschutzbeauftragten müssen (Ziel: online) der Behörde gemeldet werden
- Datenpannen müssen (Ziel: online) an die Behörde gemeldet werden. Verdächtig kann in Zukunft sein, wer keine Vorfälle meldet

Wie schon erwähnt:

- Bußgelder müssen abschreckend sein.
- Und es muss sanktioniert werden

Geänderte Rolle der Aufsichtsbehörden

- Ein geänderter Prüfungsschwerpunkt der Aufsichtsbehörden für die Zukunft wird sein „Zeig mir mal … { das Konzept | den Plan }„
  - Zitat Herr Kranig: „man muss einen Prozess im Unternehmen etabliert haben um zu erkennen, dass etwas passiert ist und wie man gedenkt dies innerhalb von 72 Std der Aufsichtsbehörde zu melden. Es ist zu spät, wenn man erst dann darüber nachdenkt, wenn etwas passiert ist.“
  - Man sollte planen "Feuerwehrübungen durchzuführen". Um z.B. Meldewege zu überprüfen.

- Datenschutzleitlinie ist von der Geschäftsführung zu definieren
  (Datenschutzziele * Datenschutz Governance Struktur => Datenschutzleitlinie)
  - DS-GVO Art 5 Abs 2 => Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).
  - Für die Aufsichtsbehörde ist es leicht zu prüfen (siehe oben "zeig mir mal").
  - Aber schwieriger ist es für Unternehmen, den Nachweis zu führen (Beweislastumkehr)

AKTUELLES AUS DER PRAXIS

Offener Mailverteiler

Es wurde ein Bußgeld wegen der Verwendung des “An:” statt des “Bcc:” Feldes in dem Fall einer Massen-E-Mail verhängt.

> “(…) Im Hinblick auf die erhebliche Anzahl der E-Mail-Adressen … ein Bußgeld verhängt.

Da in manchen Unternehmen dieser Fragestellung offensichtlich nicht die entsprechende Bedeutung beigemessen wird, … einen Bußgeldbescheid nicht gegen den konkreten Mitarbeiter, der die Mail mit offenem E-Mail-Verteiler versandt hat, erlassen, **sondern gegen die Unternehmensleitung.**”

Verschlüsselungsmethoden

Zusammenfassung

Was Sie vom heutigen Tag mitnehmen können

a. Verpflichtung auf das Datengeheimnis vornehmen
b. Datenschutzerklärung auf Ihre Web Site
c. Firmenhandys sind machbar wenn auch nicht ganz einfach BYOD ist deutlich komplexer
d. Private E-Mail und Internetnutzung am Arbeitsplatz regeln
e. Auf Datenschutz Grundverordnung vorbereiten
f. Verschlüsselung einsetzen wo immer es geht

Kontaktdaten:
Hubert Daubmeier
hubert@daubmeier.de
https://daubmeier.de

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!